Deutsch | Bedienungsanleitung

IPC-765VGA

INDOOR IP-KAMERA

mit QR-Code / VGA / WLAN / IR

PX-3722-675

IPC-765VGA

INDOOR IP-KAMERA

mit QR-Code / VGA / WLAN / IR

© 07/2013 – HA//FD//FrG – GS

INHALTSVERZEICHNIS

EINLEITUNG

Ihre neue IP-Kamera 6

Verwendung dieser Bedienungsanleitung 7
Verwendete Symbole 7
Verwendete Textmittel 7
Gliederung 8

Wichtige Hinweise zu Beginn 9
Sicherheitshinweise 9
Wichtige Hinweise zur Entsorgung 9
Konformitätserklärung 10

Produktinformationen 11

Detailsansicht 13

INSTALLATIONSANLEITUNG

Installation 15
Produktempfehlungen 15
Vorbereitung 16
Anschluss und Inbetriebnahme 18

Browser-Zugriff auf die Kamera 25

ActiveX – Steuerelemente aktiveren 27
Unter Windows 7 (und Vista) 27
Unter Windows XP 35
Sicherheitseinstellungen wiederherstellen 44

WLAN-Einstellungen 47

Verbindung einrichten 48
Weboberfläche über iPhone aufrufen 51
Kamera mit dem iPhone verbinden 51
WEP 53
WPA und WPA2 54
Verbinden 55

Montage 56

VERWENDUNG

Grundlegende Steuerung **57**

Passwort einstellen **58**

Benutzerkonten einrichten **60**

WLAN-Einstellungen **63**

Mehrere Kameras im Netzwerk verbinden **65**

Updates installieren **69**

ANHANG

Anschluss von Bewegungsmeldern **74**
Einstellungen des Alarmdienstes 74
I/O Pins 75
Alarm-Eingang aktivieren 76
I/O Verbindung bei Alarm 77

Lösung häufiger Probleme (Troubleshooting) **78**
Die Kamera wird im Netzwerk nicht erkannt 78
Das Passwort und/oder der Benutzername sind verloren gegangen. 78
Die Bilderübertragungsrate ruckelt und/oder ist von minderer Qualität 79

Basiswissen Netzwerke **80**
Hardware 80
Grundlegende Netzwerkbegriffe 81
Dienste in Netzwerken 86

Sicherheitsmaßnahmen in WLAN-Netzwerken **90**

Index **92**

Checkliste für die Konfiguration **95**

EINLEITUNG

IHRE NEUE IP-KAMERA

Sehr geehrte Kundin, Sehr geehrter Kunde,
vielen Dank für den Kauf dieser Wireless-Netzwerk-IP-Kamera, einer leistungsstarken kabellosen Netzwerkkamera für Bilder mit hoher Qualität und mit Audio vor Ort via Internetverbindung. Bitte beachten Sie die folgenden Hinweise zum Aufbau der Bedienungsanleitung und lesen Sie alle Kapitel sorgfältig durch, damit Sie Ihre neue Kamera optimal einsetzen können.

VERWENDUNG DIESER BEDIENUNGSANLEITUNG

Verwendete Symbole

	Dieses Symbol steht für mögliche Gefahren und wichtige Informationen im Umgang mit diesem Produkt. Es wird immer dann verwendet, wenn Sie eindringlich auf etwas hingewiesen werden sollen.
	Dieses Symbol steht für nützliche Hinweise und Informationen, die im Umgang mit dem Produkt helfen sollen „Klippen zu umschiffen“ und „Hürden zu nehmen“.
	Dieses Symbol wird für beispielhafte Anwendungen und Erläuterungen verwendet, die oft komplexe Vorgehensweisen veranschaulichen und begreiflich machen sollen.
	Dieses Symbol wird oftmals hinter Fachbegriffen zu finden sein, zu denen weitere Erläuterungen im Glossar zu finden sind. Das Glossar soll dabei helfen, diese Fachbegriffe für den Laien verständlich zu machen und in einen Zusammenhang zu rücken.

Verwendete Textmittel

GROSSBUCHSTABEN	Großbuchstaben werden immer dann verwendet, wenn es gilt Tasten, Anschluss- oder andere Produkt-Beschriftungen kenntlich zu machen.
Fettschrift	Fettschrift wird immer dann eingesetzt, wenn Menüpunkte oder genau so bezeichnete Ausdrücke in der Software des Produktes verwendet werden.
1. Aufzählungen 2. Aufzählungen 3. Aufzählungen	Aufzählungen werden immer dann verwendet, wenn Sie eine bestimmte Reihenfolge von Schritten befolgen sollen, oder die Merkmale des Produktes beziffert werden sollen.

Gliederung
Diese Anleitung ist in vier grundlegende Bestandteile untergliedert:

Kapitel 1: Einleitung	Erläuterungen zur Nutzung dieser Anleitung, Wichtige Hinweise zur Sicherheit im Umgang mit dem Produkt, Übersicht über das Produkt
Kapitel 2: Installation	Detaillierte Anleitung zur Installation und Inbetriebnahme der IP-Kamera und zur grundlegenden Konfiguration.
Kapitel 3: Verwendung	Hinweise zur Steuerung und den erweiterten Einstellungen der IP-Kamera
Anhang	Troubleshooting (Problemlösungen), Glossar, Konformitätserklärung und Index

WICHTIGE HINWEISE ZU BEGINN

Sicherheitshinweise

- Diese Bedienungsanleitung dient dazu, Sie mit der Funktionsweise dieses Produktes vertraut zu machen. Bewahren Sie diese Anleitung daher stets gut auf, damit Sie jederzeit darauf zugreifen können.
- Ein Umbauen oder Verändern des Produktes beeinträchtigt die Produktsicherheit. Achtung Verletzungsgefahr!
- Öffnen Sie das Produkt niemals eigenmächtig. Führen Sie Reparaturen nie selbst aus!
- Behandeln Sie das Produkt sorgfältig. Es kann durch Stöße, Schläge oder Fall aus bereits geringer Höhe beschädigt werden.
- Halten Sie das Produkt fern von Feuchtigkeit und extremer Hitze.
- Tauchen Sie das Produkt niemals in Wasser oder andere Flüssigkeiten.
- Technische Änderungen und Irrtümer vorbehalten!

Wichtige Hinweise zur Entsorgung

Dieses Elektrogerät gehört nicht in den Hausmüll. Für die fachgerechte Entsorgung wenden Sie sich bitte an die öffentlichen Sammelstellen in Ihrer Gemeinde.
Einzelheiten zum Standort einer solchen Sammelstelle und über ggf. vorhandene Mengenbeschränkungen pro Tag / Monat / Jahr entnehmen Sie bitte den Informationen der jeweiligen Gemeinde.

Konformitätserklärung
Hiermit erklärt PEARL.GmbH, dass sich das Produkt PX-3722 in Übereinstimmung mit der R&TTE-Richtlinie 99/5/EG, der Niederspannungsrichtlinie 2006/95/EG und der RoHS-Richtlinie 2011/65/EU befindet.

PEARL.GmbH, PEARL-Str. 1–3, 79426 Buggingen, Deutschland

Leiter Qualitätswesen
Dipl. Ing. (FH) Andreas Kurtasz
12. 07. 2013

Die ausführliche Konformitätserklärung finden Sie unter www.pearl.de. Klicken Sie unten auf den Link **Support (Handbücher, FAQs, Treiber & Co.).** Geben Sie anschließend im Suchfeld die Artikelnummer PX-3722 ein.

PRODUKTINFORMATIONEN

Die IP-Kamera bietet sowohl dem Heimanwender als auch professionellen Nutzern eine Vielzahl an Anwendungsgebieten. Für optimalen Schutz stehen außerdem die zum heutigen Sicherheitsstandard gehörenden Verschlüsselungsvarianten WPA und WPA2 zur Verfügung. Mit den 802.11b/g Standards erreichen Sie Datendurchsatzraten bis zu 54 MBit/s. Die externe Antenne ermöglicht hierbei einen verlustarmen Datentransfer über weite Strecken. Unter normalen Umweltbedingungen kann die Kamera im gesamten Sendegebiet Ihres WLAN-Routers arbeiten. Für die Fernüberwachung kann die Kamera Momentaufnahmen und Videos als Emails versenden oder diese sogar auf voreingestellte FTP-Server laden. Sie können auch mit Ihrem **iPhone** auf diese IP-Kamera zugreifen.

Lieferumfang
- IP-Kamera
- WLAN-Antenne
- Netzwerkkabel (RJ45)
- Netzteil
- Software-CD
- Bedienungsanleitung

Technische Daten
- 1/4"-CMOS-Sensor (Farbe)
- Auflösung: 640 x 480 Pixel (VGA)
- Nachtsicht durch 10 IR-LEDs: bis 10 m Reichweite
- Lichtempfindlichkeit: 0,5 Lux
- Sichtfeld: horizontal 280°, vertikal 90°
- Bildfrequenzrate: max. 30 fps
- Bewegungserkennung mit automatischem Bild-Versand per E-Mail
- Integriertes Mikrofon
- Unterstützt die wichtigsten Internet- und Einwahlprotokolle: HTTP, FTP, TCP/IP, SMTP, DHCP, UDP, UPnP, DDNS, PPPoE
- WLAN: Übertragungsgeschwindigkeit bis 54 Mbit/s (IEEE 802.11g) mit WEP/WPA/WPA2-Verschlüsselung
- Integrierter Web-Server
- Maße: 100 mm x 125 mm

Systemvoraussetzungen

- **Netzwerk**
  - LAN: 10 Base-T Ethernet oder 100 Base-TX Fast Ethernet
  - WLAN: IEEE 802.11b/g.

- **Computer für Webbrowser-Zugriff**
  - Betriebssystem: Microsoft Windows 2000/XP/Vista/7
  - Arbeitsspeicher: 128 MB RAM
  - Auflösung: 800 x 600 oder besser
  - Browser: Microsoft Internet Explorer (8.0 oder neuer)
  - Prozessor: Intel Pentium III 800 MHz oder besser

Angeschlossene Kameras	Prozessor	Arbeitsspeicher
1	Pentium III / 800 MHz	512 MB RAM
2 bis 4	Pentium 4 / 1,3 GHz	512 MB RAM
5 bis 8	Pentium 4 / 2,4 GHz	1 GB RAM
9 bis 16	Pentium 4 / 3,4 GHz	2 GB RAM

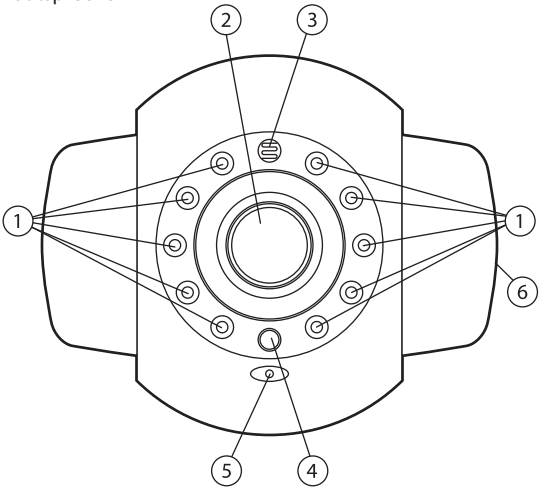
Statt eines Intel-Pentium-Prozessors kann jeweils auch ein AMD-Prozessor mit vergleichbaren Leistungswerten verwendet werden. Die hier angegebenen Daten sind die minimal benötigten Werte. Höhere Leistungswerte erleichtern in jedem Fall die Bedienung und beschleunigen die Installation und Verwendung.

HINWEIS:
Die Software der Kamera verwendet ActiveX-Steuerelemente, verwenden Sie daher nur den Internet Explorer und keine anderen Browser wie Mozilla Firefox, Apple Safari oder Google Chrome.

DETAILSANSICHT

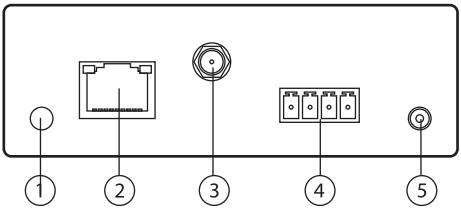
Vorderseite

1. Infrarot-LEDs
2. Linse (CMOS-Sensor mit fest integrierter Linse)
3. Lichtsensor
4. Netzwerk-LED
5. Mikrofon
6. Lautsprecher



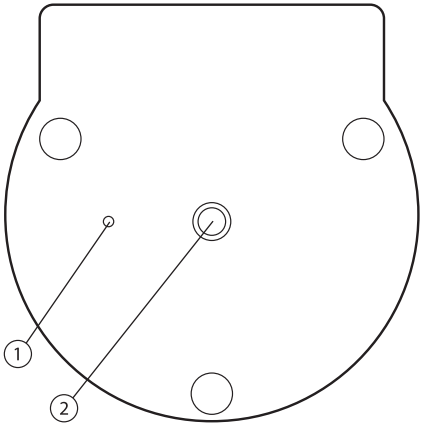
Rückseite

1. Kopfhörerausgang
2. RJ45 Ethernet-Anschluss
3. Antenne
4. I/O Alarm-Anschlüsse
5. Netzteil-Anschluss



Unterseite

1. Reset-Taste
2. Halterungsöffnung



INSTALLATIONSANLEITUNG

INSTALLATION

ACHTUNG:
Nehmen Sie die Kamera in Betrieb und versichern Sie sich, dass sowohl die LAN- als auch die WLAN-Funktion problemlos funktionieren, bevor Sie die Kamera fest montieren. Weitere Hinweise zur Montage finden Sie am Ende dieses Kapitels.

HINWEIS:
Viele der Fachbegriffe werden im Anhang „Basiswissen Netzwerke" erläutert (S. 78). Sollten dennoch Fragen bezüglich der Installation bestehen, können Sie sich gerne an die Service-Hotline Ihres Fachhändlers wenden.

Produktempfehlungen
Zusätzlich zu den unbedingt notwendigen Zubehörteilen empfehlen wir Ihnen für die Erweiterung Ihres Netzwerkes und die Verwendung der Kamera folgende Artikel, die Sie unter www.pearl.de bestellen können:

PE-5586-675	ConnecTec 10/100MBit Netzwerk-Switch 5-Port USB mit blauen LEDs
PX-6516-675	TP-LINK 54Mbit WLAN-USB-Dongle „TL-WN321G" USB2.0 (802.11g/b)
PE-4454-675	revolt Profi-Steckdosenleiste mit Netzwerkschutz

Vorbereitung

HINWEIS:
Sollten Sie sich bei den folgenden Fragen nicht sicher sein, wird empfohlen sich an einen Fachmann zu wenden. Eine Fehlkonfiguration der Kamera kann den Zugriff auf diese unmöglich machen.

Für eine reibungslose Installation der Kamera sollten Sie folgende Daten im Vorfeld recherchieren und bereithalten:

- Die Zugangsdaten Ihres Serviceproviders (Internet-Anbieters)
- Die IP-Adresse des Gateway-Routers.
- Die Art des verwendeten Netzwerks (Infrastructure oder Adhoc).
- Wird in Ihrem Netzwerk bereits ein DHCP-Server verwendet? Wenn ja – welche Adressräume deckt dieser ab?

Ferner sollten Sie folgendes im Vorfeld beachten:

- Bei der Erstinstallation muss die Kamera direkt über Kabel mit einem Router verbunden werden.
- Beseitigen Sie eventuelle Störquellen im Funktionsbereich Ihres WLAN-Routers. Hierzu gehören Funktelefone, Funküberwachungskameras und andere Geräte, die mit dem 2,4 GHz Band funktionieren.
- Verwenden Sie zwischen Kamera und Router kein Kabel, das länger als 25 m ist – bei ungünstigen Verhältnissen kann es sonst zu einem Spannungsabfall kommen und die Kamera kann keine Signale mehr übertragen.
- Schalten Sie zur Einbindung der Kamera in ein bestehendes Netzwerk alle Firewalls, Virenscanner, MAC-Adressenfilter und Verschlüsslungen Ihres Routers aus.
- Notieren Sie sich die SSID Ihres bestehenden WLAN-Netzwerks.

HINWEIS:
Im Anhang dieser Anleitung finden Sie eine Checkliste zur Installation und Inbetriebnahme. Trennen Sie die Liste mit einer Schere heraus und verwenden Sie sie, um die einzelnen Punkte abzuarbeiten.

Anschluss und Inbetriebnahme

ACHTUNG:
Beachten Sie unbedingt die Reihenfolge der nächsten Schritte und führen Sie sie genau in dieser aus.

1. Verbinden Sie die Kamera mit einem freien Ethernet-Anschluss Ihres Routers oder einem Netzwerk-Switch. Verbinden Sie dann das Netzteil mit der Stromversorgung und dem Stromanschluss der IP-Kamera-Kabelverbindung.

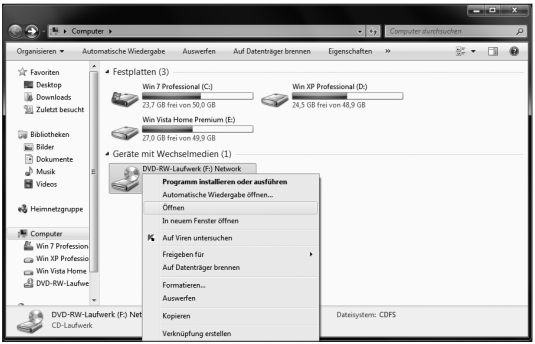
HINWEIS:
Es wird empfohlen, das Netzteil nur mit einer Mehrfach-steckdosenleiste mit integriertem Überspannungsschutz zu verbinden.

2. Starten Sie Ihren Computer und führen Sie die Softwareinstallation aus, um auf die Kamera zuzugreifen.
3. Legen Sie die mitgelieferte Software-CD in ein freies CD-/DVD-Laufwerk Ihres Computers.

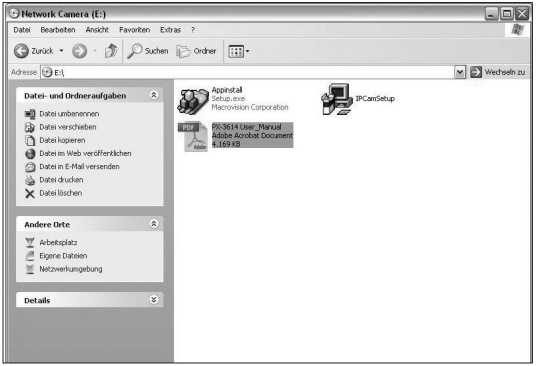
4. Wählen Sie **autorun.exe ausführen**, nachdem Windows die CD erkannt hat. Fahren Sie dann mit Schritt 5 fort.

Automatische Wiedergabe
DVD-RW-Laufwerk (F:) Network Camera
Immer für Software und Spiele durchführen:
Programm installieren oder ausführen
autorun.exe ausführen
Kein Herausgeber angegeben
Allgemeine Optionen
Ordner öffnen, um Dateien anzuzeigen
mit Windows-Explorer
Weitere Optionen für die automatische Wiedergabe in der Systemsteuerung anzeigen

Sollte die CD nicht automatisch erkannt werden, öffnen Sie Ihren **Arbeitsplatz/Computer** und wählen Sie das Laufwerk mit einem Rechtsklick aus.



Wählen Sie **Explorer/Öffnen**, um den Inhalt der CD anzeigen zu lassen.



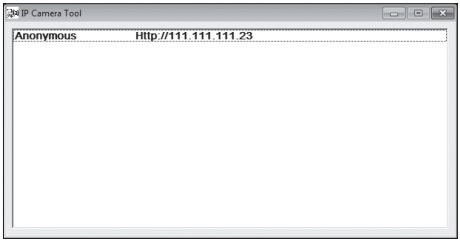
Starten Sie die Datei **IPCamSetup**.

Welcome
Welcome to the IP Camera Setup program. This program will install IP Camera on your computer.
It is strongly recommended that you exit all Windows programs before running this Setup program.
Click Cancel to quit Setup and then close any programs you have running. Click Next to continue with the Setup program.
WARNING: This program is protected by copyright law and international treaties.
Unauthorized reproduction or distribution of this program, or any portion of it, may result in severe civil and criminal penalties, and will be prosecuted to the maximum extent possible under law.
< Back
Next >
Cancel

Folgen Sie den Einstellungen des Installationsassistenten. Klicken Sie auf **Next**. Warten Sie bis die Installation abgeschlossen ist und klicken Sie dann auf **Finish**.

5. Starten Sie den IP-Finder durch einen Doppelklick auf das neue Symbol auf Ihrem Desktop.

Werkseitig ist bei der Kamera die Adressannahme per DHCP eingestellt. Im Fenster „IPFinder" werden Ihnen angeschlossene Kameras sowie deren IP und MAC Adressen angezeigt.



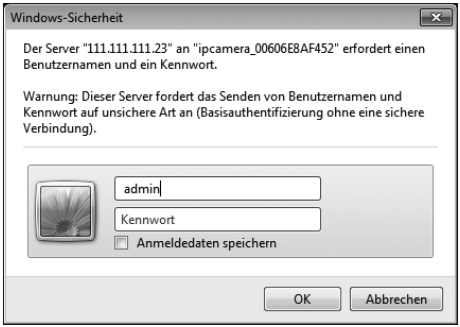
Starten Sie Ihren Internet Explorer.

HINWEIS:
Wenn Sie den Microsoft Internet Explorer verwenden, müssen im nächsten Abschnitt Active-X Steuerelemente installiert werden. Beachten Sie hierzu die Hinweise im nächsten Abschnitt. Andere Browser wie z.B. Mozilla Firefox können die benötigten ActiveX Steuerlemente nicht darstellen und zeigen nur ein begrenztes Funktionsmenü der Kamera an. Beachten Sie hierzu auch den Abschnitt „Andere Browser verwenden".

Geben Sie die angezeigte IP-Adresse in die Adresszeile Ihres Browsers ein.

BEISPIEL:
Wenn die Kamera unter der IP-Adresse „168.198.0.10" angezeigt wurde muss die Eingabe im Internet Explorer „http:// 168.198.0.10" lauten.

Im nächsten Fenster werden Sie nach dem Passwort gefragt. Geben Sie in die obere Zeile **admin** ein. Lassen Sie die zweite Zeile leer und klicken Sie auf **OK**.


Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
admin
Kennwort
Anmeldedaten speichern
OK
Abbrechen

Im Browser erscheint jetzt die Online-Steuerung der IP-Kamera. Die Kamera kann nun von jedem Computer, der mit Ihrem Netzwerk verbunden ist, angesteuert und über den Browser bedient werden.

English 簡体中文 繁體中文 España 한국어 Deutsch Français
ActiveX Mode (For IE Browser)
Sign in
Server Push Mode (For Safari,FireFox, Google Browser)
Sign in
Sign in mobile phone
attention:
case sensitive
propose using 1024 * 768 screen resolution

ACHTUNG:
Unter Windows XP wird die Kamera nicht angezeigt, bevor die benötigten Steuerelemente installiert wurden. Es erscheint lediglich die Meldung* Diese Seite kann nicht angezeigt werden*. Beachten Sie die Schritte im Abschnitt „Zugriff unter Windows XP" (S. 35) und befolgen Sie sie, um die Kamera anzeigen zu lassen und zu überprüfen, ob sie über diese IP-Adresse erreicht werden kann.

Beachten Sie die Hinweise im folgenden Abschnitt, um auf die Kamera zuzugreifen. Danach können Sie die WLAN-Einstellungen (S. 47) vornehmen und die grundlegenden Funktionen testen.

BROWSER-ZUGRIFF AUF DIE KAMERA

HINWEIS:
Führen Sie in allen aufgeführten Schritten den Internet-Explorer stets als Administrator aus.

Sie können die folgenden Browser verwenden, um auf die Kamera zuzugreifen.

Anbieter	Browser
Microsoft	Internet Explorer
Google	Chrome
Mozilla	Firefox
Macintosh	Safari

Wählen Sie zuerst in der oberen Zeile als gewünschte Sprache **Deutsch**.

Auf dem Startbildschirm der Kamera können Sie auswählen, ob Sie den Internet Explorer oder einen anderen Browser verwenden wollen (Server Push Modus).

Klicken Sie dann auf **Anmelden** unter **ActiveX Modus** oder **Server Push Modus**, je nachdem ob Sie den Internet Explorer oder einen anderen Browser verwenden.

ACHTUNG:
Im Server Push Modus sind nicht alle Funkionen der IP-Kamera verfügbar. Es ist wie hier abgebildet nur eine eingeschränkte Benutzeroberfläche verfügbar.

HINWEIS:
*Für die Verwendung des Microsoft Internet Explorers ist es notwendig weitere Einstellungen vorzunehmen. Beachten Sie hierzu den nächsten Abschnitt. Wenn Sie einen anderen Browser verwenden und **Server Push Modus** gewählt haben, überspringen Sie den nächsten Abschnitt und fahren Sie mit „WLAN-Einstellungen" (S. 47) fort.*

ACTIVEX – STEUERELEMENTE AKTIVIEREN

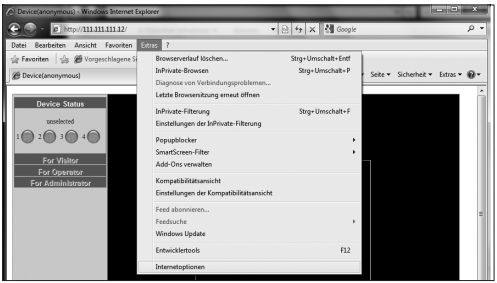
Falls Sie den Microsoft Internet Explorer verwenden und den **ActiveX Modus** ausgewählt haben, müssen vor der weiteren Verwendung einige Einstellungen vorgenommen werden.
Im folgenden Abschnitt wird der Vorgang für Windows 7 und Windows Vista beschrieben. Falls Sie Windows XP verwenden, fahren Sie mit dem Abschnitt „Unter Windows XP“ (S. 35) fort.

Unter Windows 7 (und Vista)

- **Sicherheitseinstellungen deaktivieren**

HINWEIS:
Für die Verwendung der Kamera müssen ActiveX-Steuerelemente auf Ihrem Computer installiert werden. Dies kann nur durchgeführt werden, wenn für die Dauer der Installation die Sicherheitseinstellungen des Internet Explorers deaktiviert werden. Die Sicherheits-einstellungen werden im letzen Abschnitt dieses Kapitels wiederhergestellt, damit Ihr System nicht gefährdet wird.

Öffnen Sie das Menü **Extras** Ihres Internet Explorers und wählen Sie den Menüpunkt **Internetoptionen**.

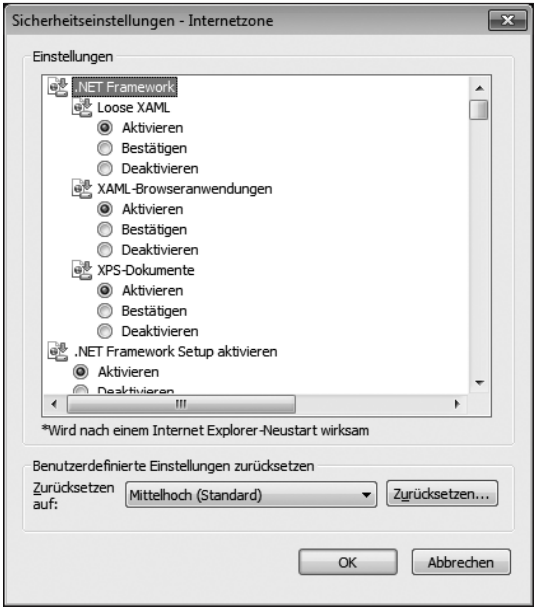


Es erscheinen die allgemeinen Internetoptionen. Klicken Sie auf **Sicherheit**.

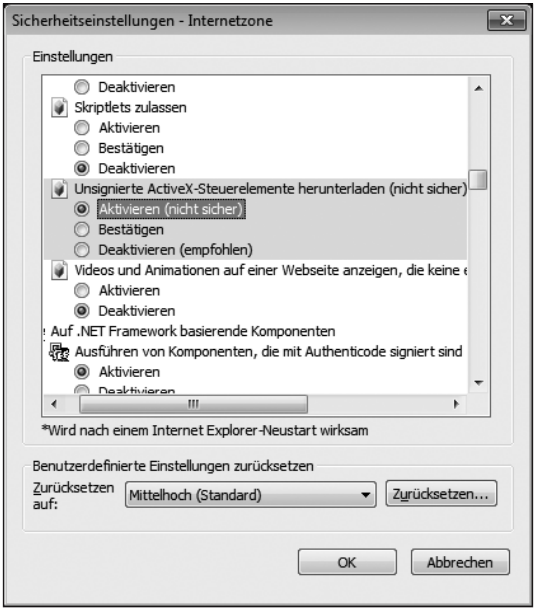
Fahren Sie mit der Maus in den Bereich **Sicherheitsstufe dieser Zone**. Die Sicherheitseinstellungen sind normalerweise auf **Mittelhoch** oder **Hoch**.

Ziehen Sie den Regler mit der Maus ganz nach unten auf **Mittel** und entfernen Sie den Haken bei **Geschützten Modus aktivieren**.

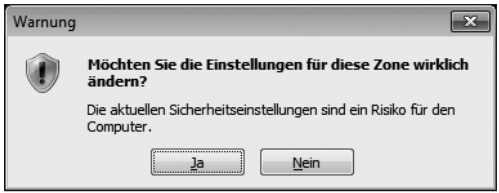
Klicken Sie auf **Stufe anpassen…**, um das Fenster **Sicherheitseinstellungen – Internetzone** zu öffnen.



Scrollen Sie nach unten, bis Sie den Punkt **Unsignierte ActiveX-Steuerlemente herunterladen** finden. Wählen Sie **Aktivieren (nicht sicher)** und klicken Sie auf **OK**.



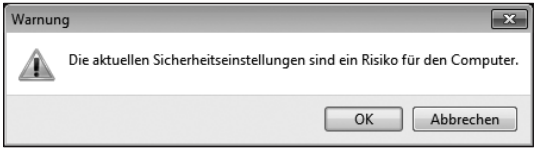
Windows verlangt eine Bestätigung, um die Sicherheitseinstellungen zu ändern. Klicken Sie auf **Ja**, um fortzufahren.


Warnung
Möchten Sie die Einstellungen für diese Zone wirklich ändern?
Die aktuellen Sicherheitseinstellungen sind ein Risiko für den Computer.
Ja
Nein

HINWEIS:
Windows zeigt Ihnen nun eine Meldung über die geänderten Einstellungen. In der Taskleiste erscheint ein neues Symbol, über das Sie die Einstellungen später wieder bequem zurücksetzen können. Weitere Informationen hierzu erhalten Sie im Abschnitt „Sicherheitseinstellungen wiederherstellen" (S. 44).

Klicken Sie auf **Übernehmen**.

Diese Sicherheitseinstellungen werden von Windows nicht empfohlen und es erscheint eine entsprechende Warnmeldung. Klicken Sie **OK**, um fortzufahren.



Die benötigten Steuerelemente können jetzt installiert werden und Sie können auf die Kamera zugreifen.

- **Zugriff auf die Kamera (Windows Vista/7)**
  Geben Sie die IP-Adresse der Kamera in die Adresszeile des Internetexplorers ein. Warten Sie bis der Login-Schirm der Kamera geladen wurde.

  Geben Sie dann Ihren USER-Namen und das Passwort ein. Werkseitig ist der USER-Name auf **„Admin“** eingestellt und **kein Passwort** festgelegt. Verwenden Sie daher beim ersten Zugriff diese Daten und klicken Sie auf **OK**.

Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
admin
Kennwort
Anmeldedaten speichern
OK
Abbrechen

HINWEIS:
Nach dem Einloggen versucht die Kamera ein ActiveX-Steuerelement zu installieren. In diesem Fall kann oben im Browser die folgende Warnmeldung erscheinen: „Möchten Sie zulassen, dass durch das folgende Programm von einem unbekannten Herausgeber Änderungen an diesem Computer vorgenommen werden?"
Klicken Sie auf die Meldung und erlauben Sie die Installation. Der Login-Schirm wird neu geladen. Geben Sie den Benutzer-Namen und das Passwort (siehe oben) erneut ein, um auf die Kamera zuzugreifen.

Sie können jetzt die grundlegende Verwendung ausprobieren und die WLAN-Einstellungen vornehmen. Fahren Sie mit „WLAN-Einstellungen" (S. 47) fort.

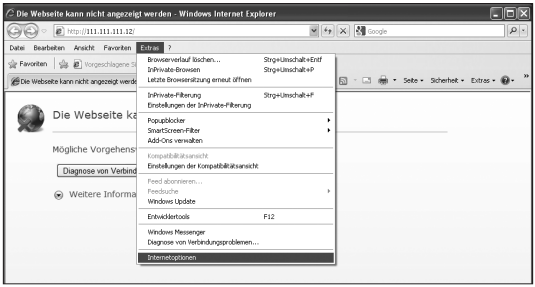
Unter Windows XP

ACHTUNG:
Für die Installation benötigen Sie eine aktuelle Version des Microsoft Internet Explorers. Vergewissern Sie sich, dass Sie alle aktuellen Updates installiert haben. Weitere Informationen erhalten Sie auf www.microsoft.com.

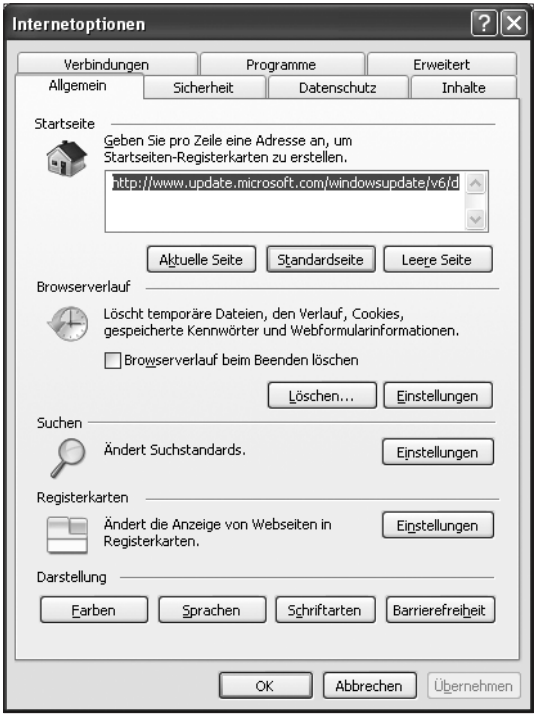
- **Sicherheitseinstellungen deaktivieren**
  Vor dem Abschluss der Installation wird der Login-Schirm der Kamera nicht angezeigt. Auch wenn Sie die richtige Adresse eingegeben haben, zeigt der Browser nur die Meldung **Diese Seite kann nicht angezeigt werden**.

HINWEIS:
Für die Verwendung der Kamera müssen ActiveX-Steuerelemente auf Ihrem Computer installiert werden. Die kann nur durchgeführt werden, wenn für die Dauer der Installation die Sicherheitseinstellungen des Internet Explorers deaktiviert werden. Die Sicherheitseinstellungen werden nach der Installation wiederhergestellt, damit Ihr System nicht gefährdet wird.

Öffnen Sie das Menü **Extras** Ihres Internet Explorers und wählen Sie den Menüpunkt **Internetoptionen**.



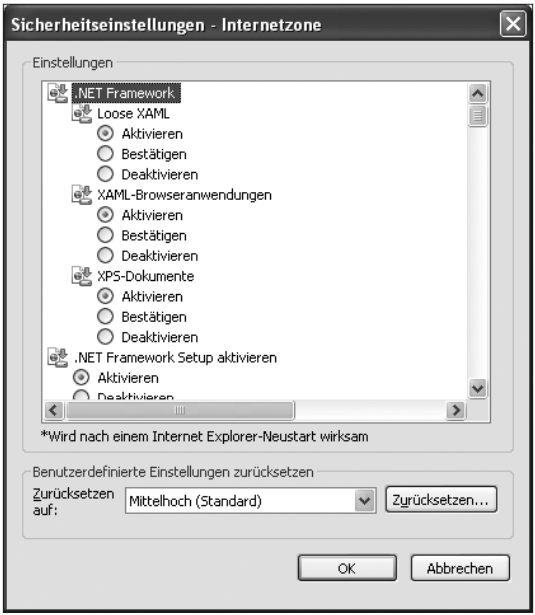
Es erscheinen die allgemeinen Internetoptionen. Klicken Sie auf **Sicherheit**.



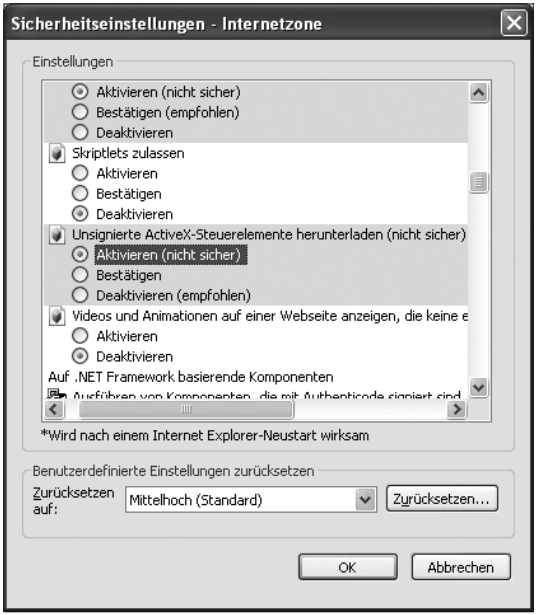
Fahren Sie mit der Maus in den Bereich **Sicherheitsstufe dieser Zone**. Die Sicherheitseinstellungen sind normalerweise auf **Mittelhoch** oder **Hoch**.

Ziehen Sie den Regler mit der Maus ganz nach unten auf **Mittel**.

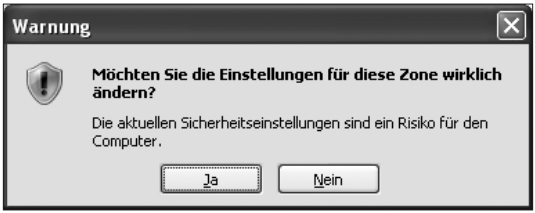
Klicken Sie auf **Stufe anpassen…**, um das Fenster **Sicherheitseinstellungen – Internetzone** zu öffnen.



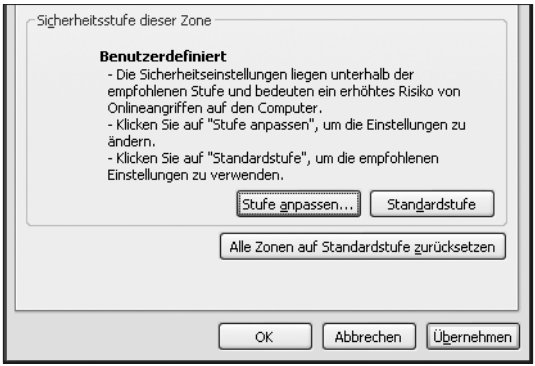
Scrollen Sie nach unten, bis Sie die Auswahlmenüs für ActiveX-Steuerelemente finden. Wählen Sie für **jeden** Punkt **Aktivieren (nicht sicher)** und klicken Sie auf **OK**.



Windows verlangt eine Bestätigung, um die Sicherheitseinstellungen zu ändern. Klicken Sie auf **Ja**, um fortzufahren.


Warnung
Möchten Sie die Einstellungen für diese Zone wirklich ändern?
Die aktuellen Sicherheitseinstellungen sind ein Risiko für den Computer.
Ja
Nein

Klicken Sie auf **Übernehmen**.


Sicherheitsstufe dieser Zone
Benutzerdefiniert
- Die Sicherheitseinstellungen liegen unterhalb der empfohlenen Stufe und bedeuten ein erhöhtes Risiko von Onlineangriffen auf den Computer.
- Klicken Sie auf "Stufe anpassen", um die Einstellungen zu ändern.
- Klicken Sie auf "Standardstufe", um die empfohlenen Einstellungen zu verwenden.
Stufe anpassen...
Standardstufe
Alle Zonen auf Standardstufe zurücksetzen
OK
Abbrechen
Übernehmen

Die benötigten Steuerelemente können jetzt installiert werden und Sie können auf die Kamera zugreifen.
Geben Sie die IP-Adresse der Kamera in die Adresszeile des Internet Explorers ein. Die Login-Seite wird jetzt angezeigt.

- **Zugriff auf die Kamera (Windows XP)**
  Geben Sie die IP-Adresse der Kamera in die Adresszeile des Internetexplorers ein. Wenn Sie die Sicherheitseinstellungen wie im vorigen Abschnitt beschrieben deaktiviert haben, wird jetzt die Login-Seite der IP-Kamera geladen.

Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
admin
Kennwort
Anmeldedaten speichern
OK
Abbrechen

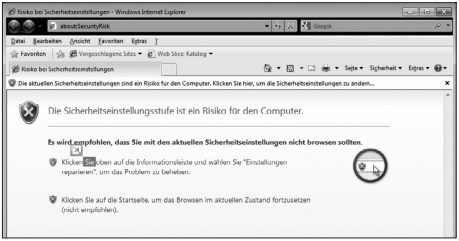
Geben Sie dann Ihren Benutzernamen und das Passwort ein. Werkseitig ist der Benutzerame auf **„Admin“** eingestellt und **kein Passwort** festgelegt. Verwenden Sie daher beim ersten Zugriff diese Daten und klicken Sie auf **Anmelden** unter **ActiveX Modus**.

Sie können jetzt die grundlegende Verwendung ausprobieren und die WLAN-Einstellungen vornehmen. Fahren Sie mit „WLAN-Einstellungen“ (S. 47) fort.

Sicherheitseinstellungen wiederherstellen

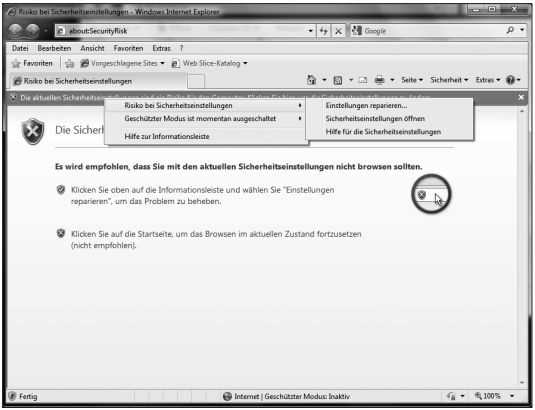
ACHTUNG:
Nach Abschluss der Installation sollten Sie unbedingt die Sicherheitseinstellungen des Microsoft Internet Explorers wiederherstellen, um Ihr System zu schützen.

Beim nächsten Start des Internet Explorers warnt Sie dieser, das die Sicherheitseinstellungen nicht ausreichend sind.

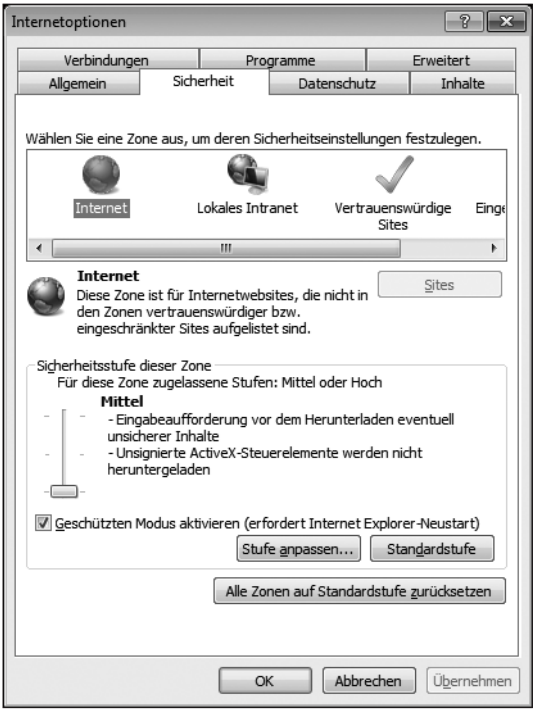

Risiko bei Sicherheitseinstellungen - Windows Internet Explorer
about:SecurityRisk
Google
Datei Bearbeiten Ansicht Favoriten Extras ?
Favoriten
Vorgeschlagene Sites
Web Slice-Katalog
Risiko bei Sicherheitseinstellungen
Seite
Sicherheit
Extras
Die aktuellen Sicherheitseinstellungen sind ein Risiko für den Computer. Klicken Sie hier, um die Sicherheitseinstellungen zu ändern...
Die Sicherheitseinstellungsstufe ist ein Risiko für den Computer.
Es wird empfohlen, dass Sie mit den aktuellen Sicherheitseinstellungen nicht browsen sollten.
Klicken Sie oben auf die Informationsleiste und wählen Sie "Einstellungen reparieren", um das Problem zu beheben.
Klicken Sie auf die Startseite, um das Browsen im aktuellen Zustand fortzusetzen (nicht empfohlen).

Folgen Sie den Anweisungen des Explorers hinter dem grünen Schild, um die Sicherheitseinstellungen wiederherzustellen.

Klicken Sie auf die Anzeige oben im Browserfenster und wählen Sie **Risiko bei Sicherheitseinstellungen → Sicherheitseinstellungen öffnen**.


Risiko bei Sicherheitseinstellungen - Windows Internet Explorer
about:SecurityRisk
Google
Datei Bearbeiten Ansicht Favoriten Extras ?
Favoriten
Vorgeschlagene Sites
Web Slice-Katalog
Risiko bei Sicherheitseinstellungen
Seite
Sicherheit
Extras
Risiko bei Sicherheitseinstellungen
Geschützter Modus ist momentan ausgeschaltet
Hilfe zur Informationsleiste
Einstellungen reparieren...
Sicherheitseinstellungen öffnen
Hilfe für die Sicherheitseinstellungen
Es wird empfohlen, dass Sie mit den aktuellen Sicherheitseinstellungen nicht browsen sollten.
Klicken Sie oben auf die Informationsleiste und wählen Sie "Einstellungen reparieren", um das Problem zu beheben.
Klicken Sie auf die Startseite, um das Browsen im aktuellen Zustand fortzusetzen (nicht empfohlen).
Fertig
Internet | Geschützter Modus: Inaktiv
100%

Wählen Sie im nächsten Fenster **Alle Zonen auf Standardstufe zurücksetzen**.



Klicken Sie auf **Übernehmen**, um den Vorgang abzuschließen. Die Kamera kann jetzt verwendet werden. Fahren Sie mit dem Abschnitt „WLAN-Einstellungen“ (S. 47) fort, wenn Sie die Kamera kabellos verwenden wollen. Gehen Sie direkt zum Abschnitt „Grundlegende Steuerung“ (S. 57), wenn Sie die Kamera mit einem Ethernetkabel betreiben wollen.

WLAN-EINSTELLUNGEN

Sie können die Kamera über das Netzwerkkabel betreiben oder mit Ihrem WLAN verbinden. Im folgenden Abschnitt wird die WLAN-Einstellung beschrieben. Wenn Sie die Kamera weiterhin per Kabel betreiben wollen, können Sie diesen Abschnitt überspringen und direkt mit „Montage“ (S. 56) fortfahren.

Damit die Kamera per WLAN betrieben werden kann, müssen zuerst die Zugangsdaten Ihres Netzwerkes eingegeben werden. Die Einstellungen können Sie nur vornehmen, während die Kamera noch per Kabel mit Ihrem Router verbunden ist.
Folgen Sie den Schritten im vorherigen Abschnitt „Anschluss und Inbetriebnahme“ und fahren Sie dann mit Punkt 1 dieses Abschnitts fort.

HINWEIS:
Versichern Sie sich, dass Ihr Router keine Whitelist verwendet, da die Kamera sich dann nicht mit dem Netzwerk verbinden kann. Sollte Ihr Netzwerk eine Whitelist verwenden, tragen Sie die IP-Adresse der Kamera in diese ein.

VERBINDUNG EINRICHTEN

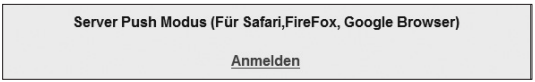
Loggen Sie sich wie in den vorherigen Abschnitten beschrieben auf der Startseite der IP-Kamera ein.
Geben Sie als Benutzername **„Admin“** und **kein Passwort** ein.
Bestätigen Sie Ihre Eingabe, indem Sie auf **OK** klicken.

Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
admin
Kennwort
Anmeldedaten speichern
OK
Abbrechen

Wählen Sie als Sprache **Deutsch** aus.

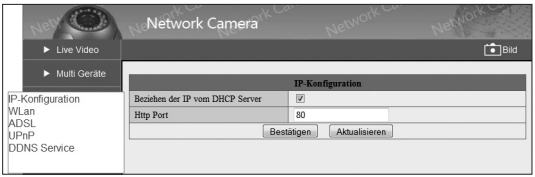
Klicken Sie auf **Anmelden** unter **Active X Modus**, wenn Sie den Microsoft Internet Explorer verwenden.

Klicken Sie auf **Anmelden** unter **Server Push Modus**, wenn Sie einen anderen Browser verwenden.



ACHTUNG:
Bei der Verwendung anderer Browser als dem Internet Explorer stehen nicht alle Funktionen der IP-Kamera zur Verfügung. Es wird ausdrücklich die Verwendung des Microsoft Internet Explorers empfohlen.

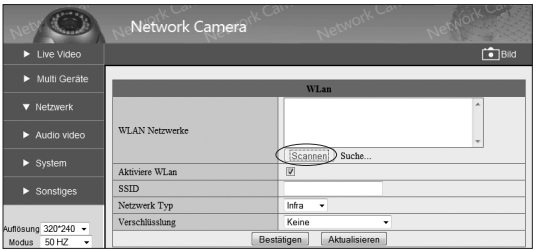
Klicken Sie auf **Netzwerk** und wählen Sie **WLAN**.



Die Seite für Netzwerkeinstellungen wird nun geladen und das Optionsmenü des Gerätes angezeigt.

Setzen Sie einen Haken hinter **Aktiviere WLan**, um das erweiterte Menü zu öffnen.

Klicken Sie auf **Scannen**. Die Kamera versucht WLAN-Netzwerke automatisch zu erkennen. Überprüfen Sie, ob Ihr Netzwerk unter **SSID** angezeigt wird. Falls dies nicht der Fall ist, geben Sie Ihre Netzwerk-SSID manuell ein.



Wählen Sie für Ihren Netzwerktyp **Infra** oder **Adhoc** aus. Für die meisten Heimnetzwerke ist **Adhoc** die richtige Auswahl.

Wählen Sie nun die **Verschlüsselung,** die von Ihrem Netzwerk verwendet wird. Für genauere Informationen hierzu beachten Sie bitte die Hinweise im Handbuch Ihres WLAN-Routers. Falls Sie keine Verschlüsselung verwenden, klicken Sie auf **Bestätigen** und fahren Sie mit Schritt „Verbinden“ (S.55) fort.

ACHTUNG:
Es wird unbedingt empfohlen Ihr Netzwerk durch eine WPA2-Verschlüsselung zu sichern. Genauere Informationen hierzu finden Sie im Anhang.

Falls Ihr Netzwerk eine WEP-Verschlüsselung verwendet, befolgen Sie die Schritte im folgenden Abschnitt „WEP“ und fahren Sie dann mit „Verbinden“ (S. 55) fort.
Falls Ihr Netzwerk eine WPA- oder WPA2-Verschlüsselung verwendet, befolgen Sie die Schritte im folgenden Abschnitt „WPA und WPA2“ und fahren Sie dann mit „Verbinden“ (S. 55) fort.
Klicken Sie auf **Bestätigen**, um die Einstellungen zu speichern und fahren Sie mit dem Abschnitt „Verbinden“ (S. 55) fort.

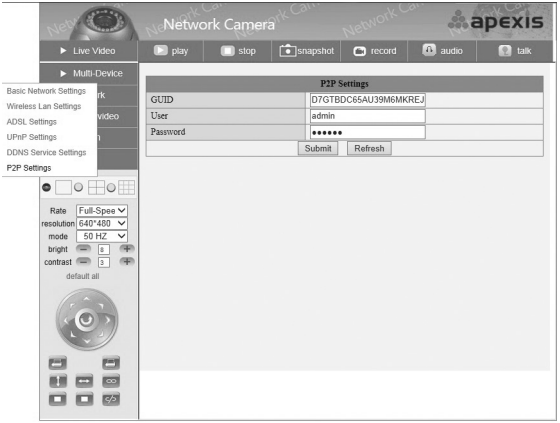
Weboberfläche über iPhone aufrufen
Sie können auf die Weboberfläche der Kamera auch über den Internetbrowser Ihres iPhones zugreifen. Rufen Sie dazu wie beschrieben die Startseite der Kamera auf und wählen Sie den entsprechenden Link aus. Im Smartphone-Modus stehen nur die Grundfunktionen der Kamera zur Verfügung.

HINWEIS:
Die Weboberfläche der Kamera funktioniert nur auf Smartphones, die Videoübertragungen über ein Netzwerk unterstützen.

Kamera mit dem iPhone verbinden
1. Installieren Sie eine geeignete App zum Scannen von QR-Codes. Entsprechende Apps gibt es kostenlos sowohl für iOS als auch für Android im App-Store bzw. dem Play-Store. Einen Tipp für geeignete Apps finden Sie auf der Produktseite unter **www.pearl.de**.
2. Scannen mit der installierten App den QR-Code an der Unterseite der Kamera.
3. Geben Sie das Passwort **000000** ein. Ab Werk ist als Standard-Passwort **000000** voreingestellt. Ändern Sie das Passwort, um einen unerwünschten Zugriff zu verhindern.

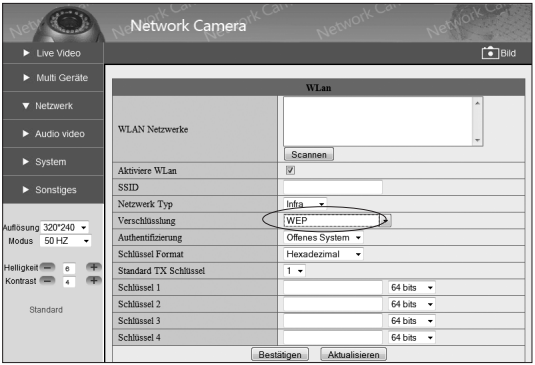
HINWEIS:
*Sie können von Ihrem iPhone aus via **EDGE**, **3G** oder **Wifi** auf die Kamera zugreifen*

- **P2P-Einstellungen**
  Klicken Sie auf **Params Settings → P2P-Settings**, um die Daten für Ihre iPhone-Verbindung zu ändern.



WEP

Mit den folgenden Schritten können Sie die IP-Kamera auf ein WEP ◙ geschütztes Netzwerk zugreifen lassen.



Wählen Sie zuerst **WEP** aus dem Dropdown-Menü, um die benötigten Eingabefelder zu öffnen.

Authentifizierung	Offenes System

Wählen Sie unter **Authentifizierung** aus, ob Sie Offenes System oder Pre-Shared Key ◙ verwenden.

Schlüssel Format	Hexadezimal

Stellen Sie hier ein, ob Ihre Netzwerkschlüssel im Hexadezimalsystem oder als ASCII-Zeichen eingegeben werden.

Standard TX Schlüssel	1

Wählen Sie hier den Schlüssel aus, der von Ihrem Netzwerk als Standard verwendet wird.

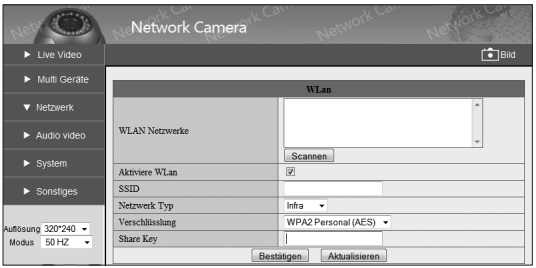
Schlüssel 1		64 bits
Schlüssel 2		64 bits
Schlüssel 3		64 bits
Schlüssel 4		64 bits

Geben Sie den Shared Key Ihres Netzwerks ein und geben Sie an, ob dieser eine 64- oder 128-Bit-Verschlüsselung verwendet. Sie müssen nur den Key angeben, dessen Nummer Sie beim vorherigen Punkt angegeben haben.

Klicken Sie auf **Bestätigen**, um die Einstellungen zu speichern und fahren Sie mit dem Abschnitt „Verbinden" im nächsten Abschnitt fort. Die Kamera startet sich neu, um die neuen Einstellungen zu laden.

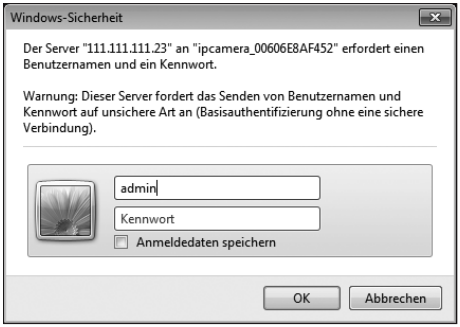
WPA und WPA2

Mit den folgenden Schritten können Sie die IP-Kamera auf ein WPA oder WPA2 geschütztes Netzwerk zugreifen lassen.



Wählen Sie den verwendeten WPA-Modus und geben Sie den Pre-Shared-Key ein. Klicken Sie auf **Bestätigen**, um die Einstellungen zu speichern und fahren Sie mit dem Abschnitt „Verbinden" im nächsten Abschnitt fort.

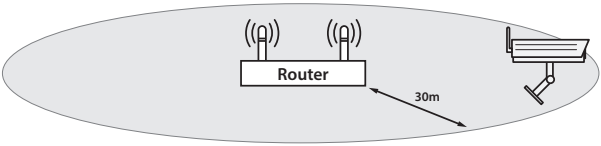
Verbinden
Nachdem die Einstellungen der vorherigen Abschnitte vorgenommen wurden, können Sie die IP-Kamera auch kabellos ansteuern. Entfernen Sie das Ethernetkabel und schrauben Sie die Antenne hinten an die IP-Kamera. Starten Sie dann Ihren Browser neu und geben Sie die IP-Adresse der Kamera erneut ein. Die Login-Seite der Kamera wird geladen.


Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
admin
Kennwort
Anmeldedaten speichern
OK
Abbrechen

Geben Sie den Benutzernamen und das Passwort erneut ein. Der Zugriff auf die Kamera erfolgt auf die gleiche Weise wie in den Abschnitten „Browserzugriff auf die Kamera“ (S. 25) beschrieben.

MONTAGE

Nachdem die IP-Kamera betriebsbereit ist und in Ihrem Netzwerk erkannt wird, kann sie aufgestellt werden. Versichern Sie sich, dass die Kamera den von Ihnen gewünschten Bereich überwachen kann und sie sich im Empfangsbereich Ihres WLAN-Routers befindet. Die maximale Reichweite für eine stabile WLAN-Verbindung beträgt 30 Meter.



VERWENDUNG

GRUNDLEGENDE STEUERUNG

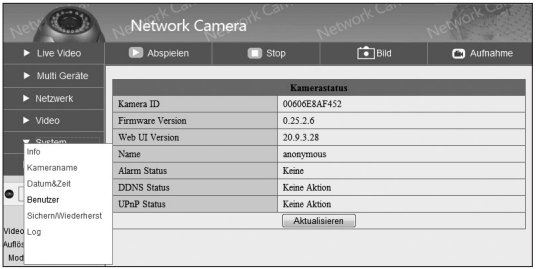
Nach dem Einloggen werden Ihnen das Kamerabild und das Bedienfeld angezeigt. Als Administrator können Sie auf den vollen Funktionsumfang der Kamera zugreifen.

1. Wiedergabe
2. Wiedergabe stoppen
3. Schnappschussauslöser
4. Videoaufnahme starten
5. Videoansicht
6. Auflösung
7. Modus
8. Helligkeit
9. Kontrast
10. Alle Werte in diesem Menü auf Werkseinstellungen setzen
11. Steuerungsfeld
12. Patroullierfunktion

PASSWORT EINSTELLEN

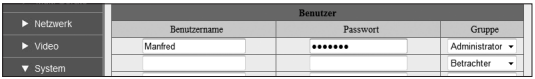
Jeder Benutzer sollte gleich zu Beginn einen neuen Benutzernamen und ein Passwort festlegen, um die Kamera vor unbefugtem Zugriff zu schützen. Befolgen Sie dafür die folgenden Schritte.

Klicken sie auf **System**.



Klicken Sie im Dropdown-Menü auf **Benutzer**.

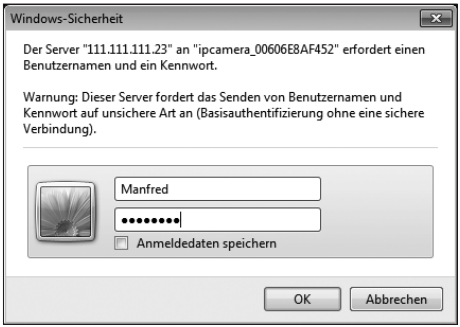
Ändern Sie im obersten Feld das Wort „admin“ indem Benutzernamen, den Sie verwenden wollen.



Tragen Sie im Feld **Password** dahinter das Passwort ein, das Sie verwenden wollen.

Klicken Sie auf **Bestätigen** um die Einstellungen zu speichern.

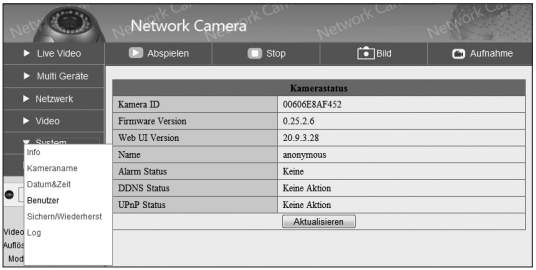
Von jetzt an werden der von Ihnen festgelegte Benutzername und das neue Passwort benötigt, um über die Login-Seite der IP-Kamera auf diese zuzugreifen.


Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
Manfred
Anmeldedaten speichern
OK
Abbrechen

BENUTZERKONTEN EINRICHTEN

Sie können Benutzerkonten mit verschiedenen Zugangsberechtigungen für die IP-Kamera anlegen.

Klicken Sie auf **System**.



Klicken Sie im Dropdown-Menü auf **Benutzer**.

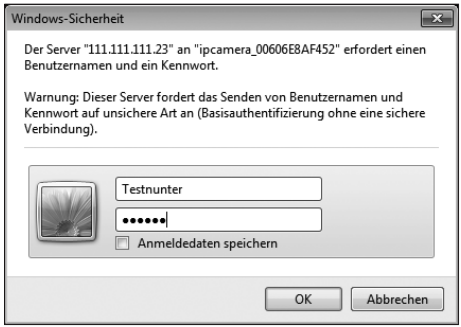
Geben Sie den gewünschten Anmeldenamen und ein Passwort ein.

Wählen Sie aus dem Dropdown-Menü die gewünschte Zugangsberechtigung und klicken Sie auf **Bestätigen**.

Betrachter	Kann lediglich die aktuelle Anzeige der Kamera betrachten
Benutzer	Kann die Anzeige starten/stoppen, Schnappschüsse machen und Aufzeichnungen starten
Administrator	Hat vollen Zugriff auf alle Einstellungen der Kamera

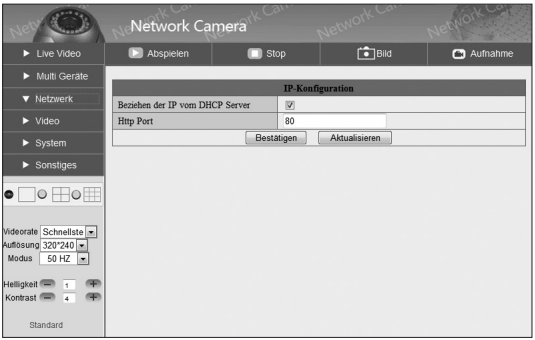
ACHTUNG:
Im Normallfall sollte nur Ihr eigenes Benutzerkonto über Administrator-Rechte verfügen.

Der neu angelegte Benutzer kann sich jetzt mit der Kamera anmelden.

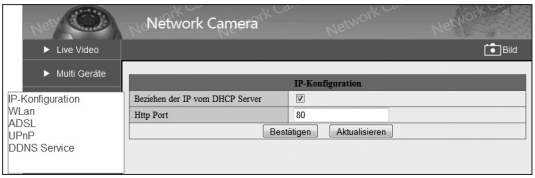

Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
Testnunter
Anmeldedaten speichern
OK
Abbrechen

WLAN-EINSTELLUNGEN

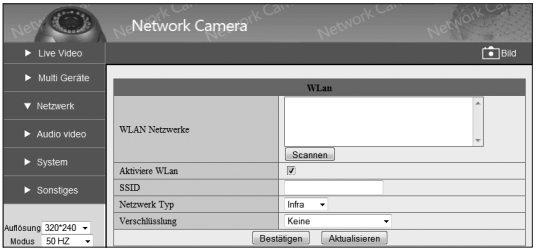
Die Kamera kann in bestehende WLAN-Netzwerke eingebunden werden. Hierzu muss sie jedoch erst per Kabel mit dem Netzwerk verbunden werden, damit die nötigen Einstellungen vorgenommen werden können. Um zu den Einstellungen zu gelangen, klicken Sie auf **Netzwerk**.



Klicken Sie dann auf den Menüpunkt **Wlan**.



Setzen Sie einen Haken bei **Aktiviere WLan**.

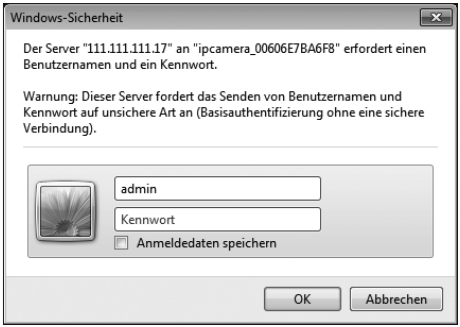


HINWEIS:
Da die Wlan-Einstellungen für die Inbetriebnahme der Kamera notwendig sind, werden diese ausführlich im Kapitel „Installation" (S. 15) behandelt.

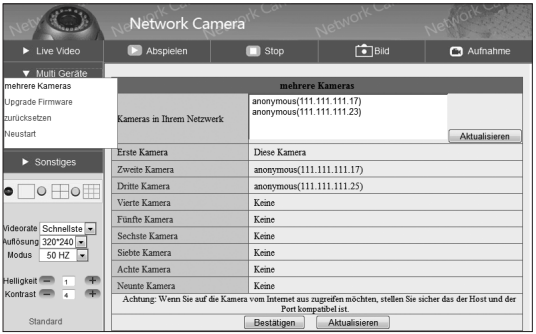
MEHRERE KAMERAS IM NETZWERK VERBINDEN

Wenn Sie mehre IP-Kameras der Serie PX-3614-675 und PX-3615-675 verwenden, können Sie bis zu 9 Kameras über ein einzelnes Browserfenster steuern. Richten Sie hierzu zuerst die anderen Kameras wie im Kapitel „Installation“ (S. 15) beschrieben ein und befolgen Sie dann die folgenden Schritte.

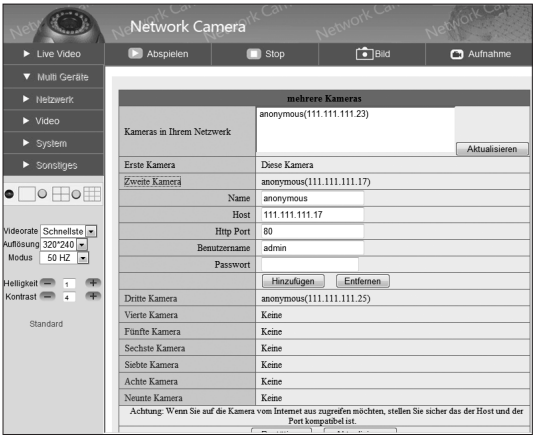
Loggen Sie sich mit der gewünschten „Hauptkamera“ ein. Welche IP-Kamera Sie hierfür auswählen, ist nicht relevant. Sie sollten aber nach der Einrichtung immer dieselbe Kamera verwenden oder die folgenden Einstellungen bei jeder Kamera in Ihrem Netzwerk verwenden.


Windows-Sicherheit
Der Server "111.111.111.17" an "ipcamera_00606E7BA6F8" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
admin
Kennwort
Anmeldedaten speichern
OK
Abbrechen

Klicken Sie auf **Multi Geräte** und wählen Sie den Menüpunkt **mehrere Kameras**.



Klicken Sie auf **Zweite Kamera**.



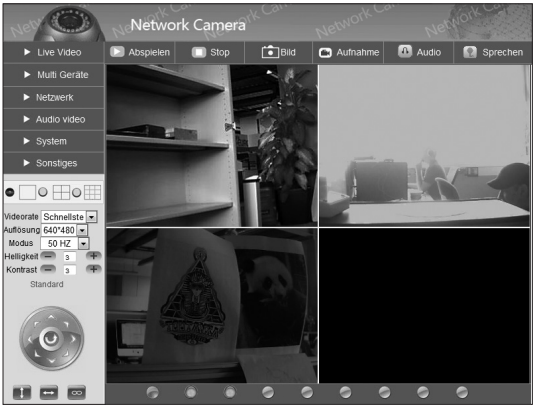
Im Feld **Kameras in Ihrem Netzwerk**, werden Ihnen die anderen Kameras angezeigt. Mit einem Doppelklick auf die Anzeige wird die IP-Adresse in das Feld **Host** kopiert. Wenn eine Kamera nicht angezeigt wird, können Sie deren Adresse auch selbst in das Feld **Host** eingeben.
Geben Sie den Namen der Kamera unter **Name** ein, falls Sie ihr einen zugewiesen haben. Ansonsten kann dieses Feld auch leer bleiben.
Geben Sie den **http-Port** der Kamera ein. Dieser ist normalerweise 80, wenn Sie ihn nicht manuell umgestellt haben.
Geben Sie den Benutzernamen und das Passwort für das Administrator-Konto der Zielkamera ein. Beachten Sie hierzu auch den Abschnitt „Passwort einstellen“ (S. 56). Klicken Sie zum Abschluss auf **Hinzufügen**.

HINWEIS:
Sie benötigen den Benutzernamen und das Passwort für die Kamera, die Sie verbinden wollen, nicht die Daten für die Kamera, die Sie gerade verwenden.

Klicken Sie auf **Live Video**. Die Kamera wird jetzt als zusätzlicher grüner Punkt in der unteren Leiste angezeigt.

Sollte eine Kamera nicht erreichbar sein, wird der Kreis orange angezeigt.

Wählen Sie eines der Mehrfachansichts-Fenster, um das Bild aller angeschlossenen Kameras zu sehen.



Mit einem Klick in das Kamerabild wechseln Sie in deren Steuerung. Beachten Sie hierzu auch den Abschnitt „Grundlegende Steuerung“ (S. 57). Mit einem Doppelklick in die Anzeige können Sie sich die Aufnahme als Vollbild anzeigen lassen. Wiederholen Sie diese Schritte, um bis zu 9 Kameras im Netzwerk miteinander zu verbinden.

HINWEIS:
Falls Sie sowohl Outdoor- als auch Indoorkameras dieser Serie miteinander verbinden, sollten Sie das Menü einer Indoorkamera für die Steuerung verwenden. Da die Indoorkameras über den Browser bewegt werden können, verfügen diese über ein erweitertes Menü, das bei deren Ansteuerung verwendet werden sollte.
Das Steuerungsfeld ist bei der Verwendung mit einer OUTDOOR-IP-Cam ohne Funktion.

UPDATES INSTALLIEREN

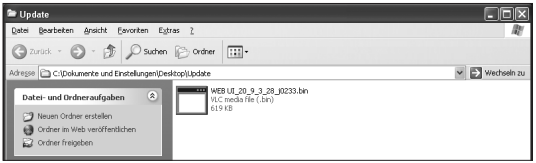
Wenn neue Firmware-Versionen verfügbar werden, können Sie diese auf **www.pearl.de** herunterladen. Diese Updates dienen der Erweiterung des Funktionsumfangs und der Behebung bekannter Fehler.

Bitten befolgen Sie die nachfolgenden Schritte exakt, da sonst kein erfolgreiches Update ausgeführt werden kann.

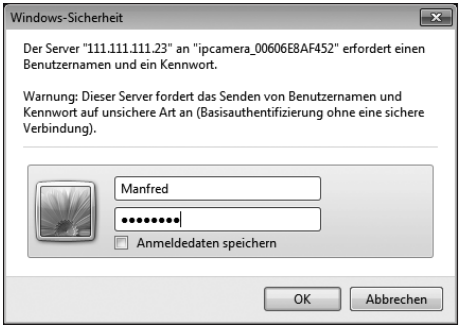
ACHTUNG:
Während des Updates darf die Stromversorgung der Kamera keinesfalls unterbrochen werden.

Klicken Sie unten auf **SUPPORT (Treiber & Co.)**. Geben Sie dann die Artikelnummer (PX-3615) in das Feld ein und klicken Sie auf **OK**, um die neuste verfügbare Software für Ihre IP-Kamera zu finden.

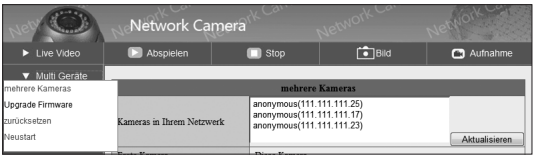
Speichern Sie die Update-Datei auf dem Desktop Ihres Computers oder in einem neuen Ordner. Es handelt sich um eine .bin-Datei. Ändern Sie niemals den Dateinamen, da das Update sonst nicht installiert werden kann.



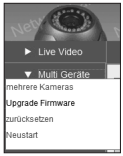
Starten Sie Ihren Internetexplorer und geben Sie die IP-Adresse Ihrer Kamera ein. Beachten Sie hierzu auch die Hinweise im vorherigen Kapitel. Warten Sie, bis der Login-Schirm angezeigt wird.


Windows-Sicherheit
Der Server "111.111.111.23" an "ipcamera_00606E8AF452" erfordert einen Benutzernamen und ein Kennwort.
Warnung: Dieser Server fordert das Senden von Benutzernamen und Kennwort auf unsichere Art an (Basisauthentifizierung ohne eine sichere Verbindung).
Manfred
Anmeldedaten speichern
OK
Abbrechen

Wählen Sie im Browserfenster der Kamera die Option **Multi Geräte**.

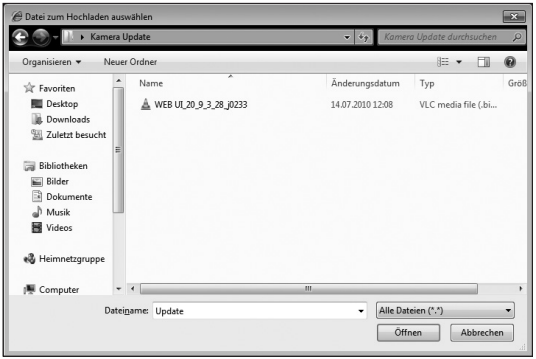


Wählen Sie den Punkt **Upgrade Firmware**.

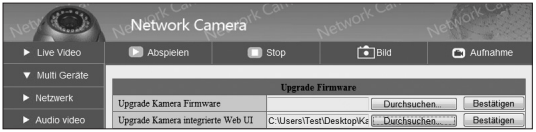


Wählen Sie **Upgrade Kamera integrierte Web UI** und klicken Sie auf **Durchsuchen** .

Warten Sie, bis sich das Fenster zur Dateiauswahl öffnet und wählen Sie die Update-Datei. Klicken Sie auf **Öffnen**.



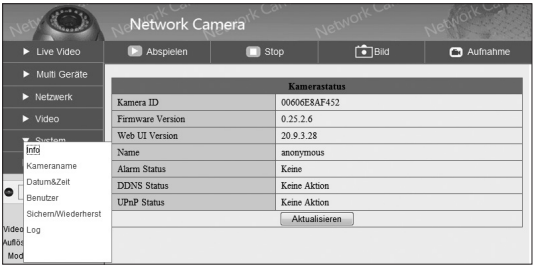
Klicken Sie **Bestätigen**.



Die Kamerasoftware versucht nun neu zu starten.

Warten Sie bis der Countdown abgelaufen ist. Starten Sie Ihren Internet Explorer neu und geben Sie die IP-Adresse der Kamera ein. Sie werden mit einem neuen Anmeldefenster begrüßt. Geben Sie wie gewohnt Ihren Benutzernamen und Ihr Passwort ein.

Die neue Firmware ist jetzt betriebsbereit und kann verwendet werden. Sie können die verwendete Firmware-Version jederzeit überprüfen, indem Sie **System** und den Menüpunkt **Info** klicken.



ACHTUNG:
Die Kamera kann beschädigt werden, wenn diese von der Stromversorgung oder Ihrem Computer getrennt wird, während das Update ausgeführt wird. Bei Schäden, die durch falsche Ausführung des Updates entstehen, entfällt der Gewährleistungsanspruch. Halten Sie sich daher genau an die hier aufgeführten Schritte.

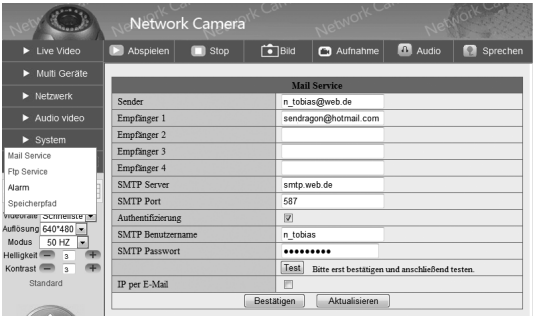
ANHANG

ANSCHLUSS VON BEWEGUNGSMELDERN

An den I/O-Anschlüssen an der Rückseite der Kamera kann ein Bewegungsmelder angeschlossen werden.

Einstellungen des Alarmdienstes

Klicken Sie auf **Sonstiges** und wählen Sie **Alarm**, um die Bewegungsmelder-Funktion einzurichten.



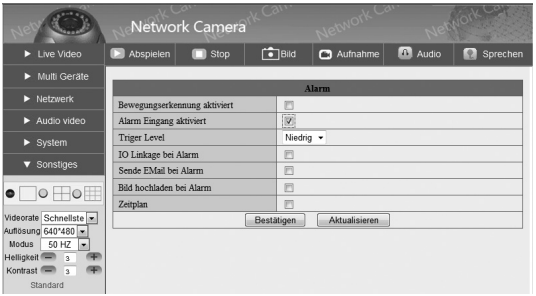
Setzen Sie einen Haken bei **Bewegungsmelder aktiviert**, um die Funktion zu verwenden.

Wenn die Bewegungserkennung aktiviert wurde, können weitere Einstellungen (wie die Empfindlichkeit und die Art des Alarms) festgelegt werden.

I/O Pins

1. Output (+5V)
2. Output
3. Alarm Input
4. Input (GND)

Alarm-Eingang aktivieren
Setzen Sie einen Haken bei **Alarm Eingang aktiviert**, um die Funktion zu verwenden.



BEISPIEL:
Sie können einen Personen-Infrarot-Sensor (PIP) für die Bewegungsmeldung anschließen. Wenn der externe Sensor ausgelöst wird, kann die IP-Kamera darauf programmiert werden, eine Email mit einem Bild zu senden oder es intern zu speichern.
Wenn Sie einen externen Alarm mit Pin 3 und Pin 4 verknüpfen, dann wird der externe Alarm aktiviert, sobald Sie das Feld bei **Alarm Eingang aktiviert** ausgewählt haben.

I/O Verbindung bei Alarm

Bei Alarm wird die I/O-Verbindung aktiviert. Pin 1 wird als Output bei Auslösen verwendet. Pin 2 wird beim Beenden verwendet.

Mit den Feldern und können Sie den Pin 1 (+5 V) manuell steuern.

HINWEIS:
Setzen Sie Haken hinter die gewünschten Alarmreaktionen. Die Kamera kann Bilder als Emails versenden, auf dem Computer speichern und auf einen Server laden. Sie müssen die jeweiligen Einstellungen zuvor bereits in den einzelnen Menüs vorgenommen haben.

LÖSUNG HÄUFIGER PROBLEME (TROUBLESHOOTING)

Die Kamera wird im Netzwerk nicht erkannt

1. Überprüfen Sie, ob die IP-Adresse der Kamera im selben Subnetz liegt wie Ihr restliches Netzwerk.
2. Versichern Sie sich, dass die der Kamera zugewiesenen IP- und Mac-Adressen nicht schon an andere Geräte Ihres Netzwerks vergeben sind.
3. Überprüfen Sie Schritt für Schritt die Netzwerkeinstellungen der IP-Kamera.
4. Versichern Sie sich, dass Ihr Router eingehende Signale von Port 80 erlaubt.
5. Überprüfen Sie, ob bei Ihrem Router Port Forwarding aktiviert ist.

Das Passwort und/oder der Benutzername sind verloren gegangen

Stellen Sie hierfür die Werkseinstellung wieder her. An der Unterseite der Kamera befindet sich eine versenkte Reset-Taste. Verwenden Sie eine Büroklammer oder einen ähnlichen Gegenstand, um diese Taste für mehrere Sekunden zu drücken. Die Kamera wird zurückgesetzt und kann wieder mit dem Benutzernamen „admin" und ohne Passwort verwendet werden.

ACHTUNG:
Durch das Wiederherstellen der Werkseinstellungen werden alle vorgenommen Einstellungen gelöscht. Alle Benutzerdaten gehen verloren, die Zugangsdaten zu Ihrem Netzwerk sind gelöscht und die IP-Kamera muss vollständig neu eingerichtet werden. Führen Sie diesen Vorgang daher nicht leichtfertig aus.

Die Bildübertragungsrate ruckelt und/oder ist von minderer Qualität

Die Übertragung wird von mehreren Faktoren wie der genutzten Bandbreite, der Anzahl der IP-Kameras, der Prozessorleistung Ihres Computers, der Anzahl der Zugriffe, von Störsignalen im WLAN (auf der 2,4 GHz Frequenz) und durch die Modus- und Helligkeitseinstellungen beeinflusst. Überprüfen Sie, ob einer dieser Faktoren ungewöhnlich hoch oder niedrig ist, um das Problem zu identifizieren. Fall Ihr Netzwerk Hubs verwendet, tauschen Sie diese durch Netzwerk-Switches aus, um eine bessere Übertragung zu sichern.

BASISWISSEN NETZWERKE

Da bei Netzwerken häufig Unklarheiten und missverständliche Begriffe auftreten, soll dieses Glossar dabei helfen, Licht ins Dunkel mancher Fachbegriffe zu bringen. Im Folgenden werden die grundlegenden Hardwarekomponenten eines herkömmlichen Heimnetzwerks ebenso dargestellt wie die verwendeten Anwendungen und Dienste.

Hardware

- **Access-Point**
  Der Zugangspunkt oder auch Access-Point ist die „Basisstation" in einem drahtlosen Netzwerk (WLAN). Diese Funktion wird häufig in Heimnetzwerken auch von einem Router übernommen.

- **DSL-Modem**
  Das DSL-Modem verbindet Ihren Computer mit dem Internet. Wenn Sie mit mehr als einem Computer über eine Leitung Zugriff auf das Internet haben wollen, benötigen Sie einen Router, der direkt hinter das DSL-Modem geschaltet wird.

- **Kabelmodem**
  Als Kabelmodem bezeichnet man das Gerät, das Daten über Fernseh-Kabelnetze überträgt und für Breitband-Internetzugänge über Kabelanschlüsse (Kabelinternet) eingesetzt wird.

- **Netzwerkkabel/Ethernetkabel**
  Hier gibt es zwei Varianten, so genannte „Patch"-Kabel und „Crossover"-Kabel. Patchkabel sind die Kabel, die am häufigsten Verwendung in Netzwerken finden. Sie werden eingesetzt um Computer mit Switches, Hubs oder Routern zu verbinden. Crossover-Kabel werden dazu eingesetzt, um zwei Computer direkt miteinander zu verbinden, ohne ein Netzwerk zu verwenden. Patchkabel sind der gängige Lieferumfang von Netzwerkprodukten.

- **Netzwerkswitch**
  Switches werden als „Knotenpunkt" von Netzwerken eingesetzt. Sie dienen dazu, mehrere Netzwerkgeräte „auf ein Kabel" im Netzwerk zusammenzuführen. Switches sind häufig zu logischen Verbünden zusammengestellt und verbinden z.B. alle Computer aus einem Büro. Koppelt man mehrere Switches, erhält man ein komplexeres Netzwerk, das einer Baumstruktur ähnelt.

- **Router**
  Router dienen zur Zugriffssteuerung von Netzwerkcomputern untereinander und regeln ebenfalls den Zugriff auf das Internet für alle im Netzwerk befindlichen Computer. Router werden sowohl rein kabelgebunden als auch als WLAN-fähige Variante vertrieben. Meist übernehmen handelsübliche Router noch Sonderfunktionen wie z.B. DHCP, QoS, Firewall, NTP,…

Grundlegende Netzwerkbegriffe

- **Adressbereich**
  Ein Adressbereich ist eine festgelegte Gruppe von IP- oder MAC-Adressen, fast diese zu einer „Verwaltungseinheit" zusammenfasst.

- **Blacklist**
  Mit einer Blacklist bezeichnet man bei Netzwerken eine Liste von Geräten, denen die Verbindung zu einem Gerät (z.B. Router) explizit nicht erlaubt ist. Alle anderen Geräte werden von dem Gerät akzeptiert, das den Zugang über die Blacklist regelt. Im Gegensatz dazu steht die so genannte Whitelist.

- **Browser**
  Browser werden Programme genannt, die hauptsächlich zur Darstellung von Webseiten genutzt werden. Die bekanntesten Browser sind Internet Explorer, Mozilla Firefox, Opera oder Google Chrome.

- **Client**
  Als Client wird jede Anwendung bezeichnet, die Daten eines Serverdienstes in Anspruch nimmt. Eine klassische Client-Server Bindung entsteht in Heimnetzwerken häufig schon bei der Vergabe von IP-Adressen im Netzwerk. Hier fordert der Computer als DHCP-Client eine gültige IP-Adresse vom DHCP-Server (meist der Router) an und erhält diese vom DHCP-Server zugeteilt.

- **IP-Adresse**
  IP-Adressen werden dazu verwendet Computer, Drucker oder andere Geräte flexibel in ein Netzwerk einzubinden. Hierbei ist zwischen globalen und privaten IP-Adressen zu unterscheiden. Globale IP-Adressen werden von den einzelnen Internet-Anbietern oftmals dynamisch (DHCP) vergeben. Sie dienen dazu, Ihr Heimnetzwerk oder auch nur den einzelnen Computer gegenüber dem Internet erreichbar zu machen. Private IP-Adressen werden im Heimnetzwerk entweder statisch („von Hand") zugewiesen oder dynamisch (DHCP) vom Anwender selbst vergeben. IP-Adressen ordnen ein spezielles Gerät eindeutig einem bestimmten Netzwerk zu.

  Beispiel:
  IP-Adressen sind die bekanntesten Adressierungen im Netzwerk und treten in folgender Form auf:
  192.168.0.1

- **ISP**
  ISP ist die Abkürzung für „Internet Service Provider". Dieser Begriff wird für Stellen verwendet, die einem Netzwerk oder Einzelcomputer den Zugang zum Internet anbieten. In Deutschland ist der wohl bekannteste ISP T-Online, aber auch Anbieter wie Freenet, Arcor, 1&1 oder KabelDeutschland gehören zu den ISPs.

- **LAN**
  LAN (Local Area Network) bezeichnet ein Netzwerk aus Computern und anderen Netzwerkgeräten, die über einen gemeinsamen Adressbereich verfügen und damit zu einer Struktur zusammengefasst werden.

- **Passphrase**
  Mit dem Begriff Passphrase wird ein Schlüsselwort oder -satz umschrieben, der als Sicherheitsabfrage bei der Verbindung zu WPA-/WPA2-verschlüsselten Netzwerken eingegeben werden muss.

- **Port**
  Als Port wird eine Softwareschnittstelle bezeichnet, die es einzelnen Anwendungen auf Ihrem Computer ermöglicht, mit den Anwendungen eines Anbieters zu kommunizieren. Hier wird hauptsächlich zwischen zwei Protokollen unterschieden: TCP und UDP.

  Beispiel:
  Die häufigste Internet Anwendung ist ein Browser (Internet Explorer, Mozilla Firefox, usw.), der meist über den TCP-Port 80 mit den Servern der Webseiten-Anbieter kommuniziert.

- **Protokoll**
  Protokolle im Netzwerk sind Standards für Datenpakete, die Netzwerkgeräte untereinander austauschen, um eine eindeutige Kommunikation zu ermöglichen.

- **Pre-Shared Key**
  Mit Pre-Shared Key („vorher vereinbarter Schlüssel") oder kurz PSK bezeichnet man ein Verschlüsselungsverfahren, bei denen die verwendeten Schlüssel vor der Verbindung beiden Teilnehmern bekannt sein müssen (siehe auch WPA/WPA2.

- **MAC-Adresse**
  Als MAC-Adresse bezeichnet man die physikalische Adresse einer Netzwerkkomponente (z.B. Netzwerkkarte, WLAN-Dongle, Drucker, Switch). MAC-Adressen sind entgegen IP-Adressen immer eindeutig zuordenbar. MAC-Adressen von anderen verbundenen Netzwerkgeräten werden von den einzelnen Geräten jeweils in einer so genannten ARP-Tabelle gespeichert. Diese ARP-Tabellen können zur Fehlersuche dienen, falls ein Gerät ohne IP-Adresse (z.B. Switch) im Netzwerk keine Funktion zeigt.

Beispiel:
Eine MAC-Adresse sieht z.B. so aus: 00:00:C0:5A:42:C1

- **Sichere Passwörter**
  Unter sicheren Passwörtern versteht man Passwörter, die bestimmte Bedingungen erfüllen, um von Angreifern nicht mit einfachsten Mitteln entschlüsselt werden zu können. Sichere Passwörter sollten generell eine bestimmte Mindestlänge aufweisen und mehrere Sonderzeichen beinhalten. Als Faustregel gilt hier: Je länger das Passwort ist und je mehr Sonderzeichen es beinhaltet, desto sicherer ist es gegen Entschlüsselung.

- **SSID**
  SSID (Service Set Identifier) steht für die Bezeichnung, die für ein WLAN-Netzwerk verwendet wird. Diese SSID wird meist per Broadcast (siehe UDP ↘) öffentlich ausgesendet, um das Netzwerk für mobile Geräte „sichtbar" zu machen.

- **Subnetz**
  Subnetze sind eine Zusammenfassung von einzelnen IP-Adressen ↘ zu Netzwerkstrukturen. So werden meist Computer einer Abteilung im Büro in einem Subnetz zusammengefasst, während die Computer einer anderen Abteilung in einem weiteren Subnetz zusammengefasst sind. Daher sind Subnetze eine reine Strukturierungsmaßnahme. Eine Angabe des Subnetzraumes wird immer in Zusammenhang mit der Vergabe einer IP-Adresse durchgeführt. Im Heimbereich werden normalerweise keine speziellen Subnetze eingerichtet. Daher ist bei Windows-Systemen als Subnetz-maske die 255.255.255.0 voreingestellt. Dadurch stehen die IP-Adressen xxx.xxx.xxx.1 bis xxx.xxx.xxx.254 zur Verfügung.

- **TCP (Transmission Control Protocol)**
  Das TCP-Protokoll wird dazu verwendet, gezielt Informationen von einem speziellen Gegenüber abzufragen (siehe Beispiel bei Port ↘)

- **UDP (User Datagram Protocol)**
  Das UDP-Protokoll ist ein so genanntes „Broadcast"-Protokoll. Broadcast wird im englischen auch für Radio- oder TV-Sendungen verwendet. Ganz ähnlich arbeitet dieses Protokoll. Es wird verwendet, um Datenpakete an alle im Netzwerk erreichbaren Geräte zu senden und im Weiteren auf Rückmeldung dieser Geräte zu warten. Das UDP-Protokoll wird meist dann von Anwendungen eingesetzt, wenn unsicher ist, ob eine entsprechende Gegenstelle im Netzwerk vorhanden ist.

- **uPNP**
  Mit diesem Begriff wird das „universal Plug and Play"-Protokoll bezeichnet. Dieses Protokoll wird hauptsächlich dazu verwendet, Drucker und ähnliche Peripheriegeräte über ein Netzwerk ansteuern zu können.

- **Verschlüsselung**
  Verschlüsselungsmechanismen werden in Netzwerken dazu eingesetzt, Ihre Daten vor fremdem Zugriff abzusichern. Diese Verschlüsselungsmechanismen funktionieren ähnlich wie bei einer EC-Karte. Nur mit dem richtigen Passwort (der richtigen PIN) können die Daten entschlüsselt werden.

- **VPN**
  VPN (Virtual Private Network) steht für eine Schnittstelle in einem Netzwerk, die es ermöglicht, Geräte an ein benachbartes Netz zu binden, ohne dass die Netzwerke zueinander kompatibel sein müssen.

- **WAN**
  WAN (Wide Area Network) bezeichnet ein Netzwerk aus Computern und anderen Netzwerkgeräten, die über größere Entfernungen und aus vielen Bestandteilen zusammengefasst werden. Das bekannteste Beispiel ist das „Internet", jedoch kann ein WAN auch nur aus zwei räumlich voneinander getrennten LANs bestehen.

- **Whitelist**
  Mit einer Whitelist bezeichnet man bei Netzwerken eine Liste von Geräten, denen die Verbindung zu einem Gerät (z.B. Router) explizit erlaubt ist. Alle anderen Geräte werden von dem Gerät abgewiesen, das den Zugang über die Whitelist regelt. Im Gegensatz dazu steht die so genannte Blacklist.

Dienste in Netzwerken

- **DHCP (Dynamic Host Configuration Protocol)**
  Mit DHCP wird die dynamische Verteilung von IP- Adressen in Netzwerken bezeichnet. Dynamisch sind diese Adressen deshalb, weil Sie jederzeit ohne größeren Aufwand neu vergeben werden können. Man kann dynamische IP-Adressen auch als geliehene IP-Adressen bezeichnen. Diese geliehenen IP-Adressen werden mit einem „Verfallsdatum" versehen – der so genannten „Lease Time". Ein Computer wird am DHCP-Server nur dann nach einer neuen IP-Adresse anfragen, wenn sein „Lease" abgelaufen ist. Dies ist allerdings auch eine mögliche Fehlerquelle, da es hier zu Unstimmigkeiten zwischen DHCP-Server und DHCP-Clients kommen kann.

HINWEIS:
Windows Computer sind standardmäßig als DHCP-Client eingestellt, um einen einfachen Anschluss an ein Heimnetzwerk zu ermöglichen.

- **DNS (Domain Name Server)**
  DNS ist ein Serverdienst, der die Übersetzung von IP-Adressen in gängige Internet-Adressen übernimmt. So wird z.B. aus www.google.de die IP-Adresse: 74.125.39.105. Werden Sie während einer Konfiguration aufgefordert, die DNS-IP-Adresse einzugeben, ist damit immer die Adresse desjenigen Servers gesucht, der den DNS-Serverdienst anbietet. DNS-Server werden aus Gründen der Ausfallsicherheit meist doppelt angegeben und als Primärer DNS (oder DNS1) bzw. Sekundärer DNS (oder DNS2) bezeichnet.

- **Filter**
  Siehe auch Firewall

- **Firewall**
  Eine Firewall ist ein Sicherungsmechanismus, der meist auf Routern als Serverdienst läuft, jedoch bereits in Windows (seit XP) integriert ist. Sie erlaubt nur Zugriffe auf voreingestellte Ports, blockt vorher konfigurierte IP-Adressen und soll generell schädliche Angriffe auf Ihr Netzwerk verhindern.

- **FTP/NAS (File Transfer Protocol/ Network Access Storage)**
  FTP ist ein Serverdienst, der hauptsächlich zum Transfer von Dateien verwendet wird. Dieser Dienst ermöglicht es auf unkomplizierte Art und Weise Dateien von einem Computer auf einen entfernt stehenden anderen Computer ähnlich dem Windows Explorer zu übertragen. So genannte NAS-Server setzen ebenfalls häufig diesen Dienst ein, um einen Zugriff aus dem gesamten Netzwerk auf eine Festplatte zu erlauben.

- **(Standard-) Gateway**
  Als Gateway wird die Schnittstelle bezeichnet, die es den Computern im privaten Netzwerk ermöglicht mit Computern außerhalb zu kommunizieren. Es ist in diesem Sinne mit Ihrem Router gleichzusetzen. Das Gateway sammelt und sendet Anfragen der Clients und leitet diese weiter an die entsprechenden Server im Internet. Ebenso verteilt das Gateway die Antworten der Server wieder an die Clients, die die Anfrage gestellt hatten.

- **HTTP/Webserver (Hypertext Transfer Protocol)**
  Dieser Dienst ist das, was in der Öffentlichkeit als „Das Internet" bezeichnet wird. Jedoch handelt es sich hier bei nur um eine Vereinfachung, da das Internet an sich eine übergeordnete Struktur ist, die nahezu alle Serverdienste beinhaltet. HTTP wird zum Transfer und der Darstellung von Webseiten verwendet.

- **Mediastreams**
  Diese Gruppe von Serverdiensten wird von vielfältigen Geräten und Anbietern verwendet. Die bekanntesten Beispiele sind Internet-Radiosender, Video-On-Demand und IP-Kameras. Diese Streams nutzen teils unterschiedliche Protokolle und Protokollversionen. Daher kann es hier durchaus einmal zu Inkompatibilitäten zwischen Server und Client kommen.

- **NTP**
  NTP (Network Time Protcol) bezeichnet ein Protokoll, mit dem Computer über das Netzwerk ihre Datums- und Zeiteinstellungen abgleichen können. Dieser Dienst wird von weltweit verteilten Servern bereitgestellt.

- **PPPoE**
  PPPoE steht für PPP over Ethernet und bezeichnet Verwendung des Netzwerkprotokolls Point-to-Point Protocol (PPP) über eine Ethernet-Verbindung. PPPoE wird in Deutschland hauptsächlich in Verbindung mit ADSL-Anschlüssen verwendet. ADSL bedeutet Asynchrones DSL und steht für die Verwendung einer Leitung für Telefon und Internet. ADSL ist Standard in Deutschland. Hauptgrund für die Verwendung von PPPoE ist die Möglichkeit, Authentifizierung und Netzwerkkonfiguration (IP-Adresse, Gateway) auf dem schnelleren Ethernet zur Verfügung zu stellen.

- **Samba/SMB**
  Mit diesen Begriffen ist ein Serverdienst gemeint, der speziell in Windows Netzwerken verwendet wird. Dieser Service ermöglicht ebenfalls den schnellen und einfachen Zugriff auf Dateien die sich auf anderen Computern befinden (in so genannten „freigegebenen Ordnern"). Jedoch ist dieser Dienst auf Heimnetzwerke begrenzt und kann nur in Ausnahmefällen auch über das Internet in Anspruch genommen werden.

- **Server/Serverdienst**
  Ein Server ist immer als Anbieter von Netzwerkdiensten zu sehen. Einzelne Anwendungen werden auch als Serverdienst bezeichnet. Die bekanntesten Serverdienste sind Webserver, DHCP oder E-Mail Server. Mehrere solche Dienste können auf einem Computer oder anderen Geräten (z.B. Routern) gleichzeitig verfügbar sein. Server werden auch Computer genannt, deren ausschließliche Funktion darin besteht Serverdienste anzubieten und zu verwalten.

- **Statische Adressvergabe**
  Bei der statischen Adressvergabe sind alle Netzwerkadressen eines Netzwerkes fest vergeben. Jeder einzelne Client (Computer) des Netzwerks hat seine feste IP-Adresse, die Subnetzmaske, das Standard-Gateway und den DNS-Server fest eingespeichert und muss sich mit diesen Daten beim Server anmelden.
  Ein neuer Client (Computer) muss erst mit einer gültigen, noch nicht vergebenen IP-Adresse und den restlichen Daten ausgestattet werden, bevor er das Netzwerk nutzen kann. Manuelle Adressvergabe ist besonders bei Netzwerkdruckern oder ähnlichen Geräten sinnvoll, auf die häufig zugegriffen werden muss, oder in Netzwerken, die besonders sicher sein müssen.

- **WEP und WPA**
  Wired Equivalent Privacy (WEP) ist der ehemalige Standard-Verschlüsselungsalgorithmus für WLAN. Er soll sowohl den Zugang zum Netz regeln als auch die Vertraulichkeit der Daten sicherstellen. Aufgrund verschiedener Schwachstellen wird das Verfahren als unsicher angesehen. Daher sollten WLAN-Installationen die sicherere WPA-Verschlüsselung verwenden. Wi-Fi Protected Access (WPA) ist eine modernere Verschlüsselungsmethode für ein WLAN. Sie wurde als Nachfolger von WEP eingeführt und weist nicht deren Schwachstellen auf.

SICHERHEITSMASSNAHMEN IN WLAN-NETZWERKEN

An erster Stelle sollten der Verzicht von WEP und der Einsatz von WPA oder WPA2 stehen. Dieses Ziel lässt sich in vielen Fällen bereits durch ein Treiber- oder Firmwareupdate erreichen. Lässt sich der Einsatz von WEP nicht vermeiden, sollten folgende grundlegende Behelfsmaßnahmen beachtet werden, um das Risiko von Angriffen fremder Personen auf das WLAN zu minimieren:

- Aktivieren Sie auf alle Fälle den Passwortschutz! Ändern Sie ggf. das Standard-Passwort des Access Points.
- Wenn Sie die WEP-Verschlüsselung verwenden, weil eines der angeschlossenen Geräte WPA oder WPA2 (dringend empfohlen) nicht unterstützt wird, sollte der WEP-Schlüssel mindestens 128 Bit lang sein und eine lose Kombination aus Buchstaben, Ziffern und Sonderzeichen darstellen.
- Aktivieren Sie die Zugriffskontrollliste (ACL = Access Control List), um vom Access Point nur Endgeräte mit bekannter MAC-Adresse zuzulassen. Beachten Sie, dass sich eine MAC-Adresse aber mittels Treiber beliebig einstellen lässt, sodass eine mitgelesene zugelassene MAC-Adresse leicht als eigene ausgegeben werden kann.
- Verwenden Sie eine sinnvolle SSID: Die SSID des Access Points sollte keine Rückschlüsse auf Ihren Namen, verwendete Hardware, Einsatzzweck und Einsatzort zulassen.
- Umstritten ist die Deaktivierung der SSID-Übermittlung (Broadcasting). Sie verhindert das unabsichtliche Einbuchen in das WLAN, jedoch kann die SSID bei deaktiviertem Broadcasting mit einem so genannten Sniffer (Gerät zur LAN-Analyse) mitgelesen werden, wenn sich etwa ein Endgerät beim Access Point anmeldet.
- WLAN-Geräte (wie der Access Point) sollten nicht per WLAN konfiguriert werden, sondern ausschließlich über eine kabelgebundene Verbindung.
- Schalten Sie WLAN-Geräte stets aus, wenn Sie sie nicht benutzen.
- Führen Sie regelmäßige Firmware-Updates vom Access Point durch, um sicherheitsrelevante Aktualisierungen zu erhalten.

- Beeinflussen Sie die Reichweite des WLANs durch Reduzierung der Sendeleistung bzw. Standortwahl des WLAN Gerätes (Dies dient allerdings nicht der aktiven Sicherheit, sondern begrenzt lediglich den möglichen Angriffsbereich.)

All diese Sicherheitsmaßnahmen dürfen aber nicht darüber hinwegtäuschen, dass sie letztlich keinen wirklichen Schutz beim Einsatz von WEP bedeuten. Ein erfolgreicher Angriff auf die WEP-Verschlüsselung ist trotz all dieser Vorkehrungen mit den richtigen technischen Voraussetzungen innerhalb von 5 bis 10 Minuten mit ziemlicher Sicherheit erfolgreich.

INDEX

A
Access-Point 78
ActiveX Modus 27
ActiveX – Steuerelemente aktiveren 27
Adressbereich 81
Adressvergabe 89
Anhang 74

B
Basiswissen Netzwerke 80
Benutzerkonten 60
Blacklist 81
Browser 25, 81
Browser-Zugriff 25

C
Checkliste 96
Chrome 25
Client 82

D
Detailsansicht 13
DHCP 86
Dienste in Netzwerken 86
DNS 86
DSL-Modem 80

E
Entsorgung 9

F
Filter 87
Firefox 25
Firewall 87
Firmware 69
FTP 87

G
Gateway 87
Gliederung 8
Grundlegende Netzwerkbegriffe 81

H
Hardware 80
HTTP 87

I
Inbetriebnahme 18
Installation 15
Internet Explorer 25
IP-Adresse 16, 82
ISP 82

K
Kabelmodem 80
Konformitätserklärung 10

L
LAN 82

M
MAC-Adresse 83
Mediastreams 88
Montage 56

N
NAS 87
Netzwerkkabel/Ethernetkabel 80
Netzwerkswitch 81
NTP 88

P
Passphrase 83
Passwort 58
Passwörter 84
Port 83
PPPoE 88
Pre-Shared Key 83
Protokoll 83

R
Router 81

S
Safari 25
Samba 88
Server 89
Sichere Passwörter 84
Sicherheit 9
SMB 88
Sprache 25
SSID 16, 84
Steuerung 57
Subnetz 84
Symbole 7
Systemvoraussetzungen 12

T
TCP 84
Textmittel 7
Troubleshooting 78

U
UDP (User Datagram Protocol) 85
Updates 69
uPNP 85

CHECKLISTE FÜR DIE KONFIGURATION

Aufgabe	Erledigt
Funkkameraüberwachung ausschalten	
Schnurlostelefon ausschalten	
Sonstige Geräte mit 2,4 GHz ausschalten	
Stromversorgung mit Überspannungsschutz sichern	
Firewall am Computer ausstellen	
Virenscanner am Computer ausschalten	
MAC-Adressenfilter am vorhandenen Router ausschalten	

Notwendige Daten	Kommentar
Netzwerk SSID	
IP – Gateway	
IP – DNS-Server	
DHCP Range	
Subnetzmaske	
IP – Internetzugang	
IP – Timeserver (wenn vorhanden)	
Passwort – Internetzugang	
Passwort – WLAN	
IPs von vorhandenen Servern (wenn vorhanden)	
IP – Watchdog (wenn vorhanden)	
IP – Log-Server (wenn vorhanden)	
IP – virtuelle DMZ (wenn vorhanden)	

Dieses Produkt enthält Software, welche ganz oder teilweise als freie Software den Lizenzbedingungen der GNU General Public License, Version 2 (GPL) unterliegt.

Den Quellcode der Software erhalten Sie unter *http://www.pearl.de/support/* unter dortiger Eingabe der Artikelnummer; wir senden Ihnen auf Anforderung (gerne unter unter *opensource@pearl.de*) den SourceCode auch auf einem handelsüblichen Datenträger, dessen Herstellungskosten wir im Gegenzug geltend machen; den vollständigen Lizenztext ersehen Sie nachfolgend. Näheres, insbesondere auch dazu, warum es keine offizielle deutsche Übersetzung der Lizenzbedingungen gibt, erfahren Sie unter *http://www.gnu.org/licenses/gpl-2.0.html*.
Da es sich um freie Software handelt, schließen die Entwickler dieser Software die Haftung, soweit gesetzlich zulässig, aus.
Bitte beachten Sie, dass die Gewährleistung für die Hardware davon natürlich nicht betroffen ist und in vollem Umfang besteht.
Weitere Fragen beantworten wir Ihnen gerne unter *opensource@pearl.de*.

GNU GENERAL PUBLIC LICENSE

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.
51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble
The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Lesser General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source

code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.
We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.
Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

1. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The „Program", below, refers to any such program or work, and a „work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term „modification".) Each licensee is addressed as „you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

2. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

   You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

3. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

   a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.
   b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.
   c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

   These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the

whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

4. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

   a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code, to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

   c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

   The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

5. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

6. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

7. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

8. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

   If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole

is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

9. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

10. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

    Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and „any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

11. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

1. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM „AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

2. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the „copyright" line and a pointer to where the full notice is found.

one line to give the program's name and an idea of what it does.
Copyright (C) ***yyyy name of author***

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the

License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 51 Franklin Street, Fifth Floor, Boston, MA 02110-1301, USA.
Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author
Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands *`show w'* and *`show c'* should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than *`show w'* and *`show c'*; they could even be mouse-clicks or menu items - whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a „copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

***signature of Ty Coon**, 1 April 1989*
Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Lesser General Public License instead of this License.